UNIVERSIDAD PABLO DE OLAVIDE

Doctorado en Ciencias Jurídicas y Políticas

TEMA: EL CONTENIDO ESENCIAL DEL DERECHO A LA PROTECCION DE DATOS PERSONALES EN EL ECUADOR A LA LUZ DE LOS MODELOS EUROPEO, NORTEAMERICANO Y LATINOAMERICANO

POR: LORENA NARANJO GODOY

SEVILLA, 22 DE NOVIEMBRE DEL 2019

DEDICATORIA

Todos tenemos sueños que queremos convertirlos en realidad. Estos contemplan renuncias y sacrificios. La recompensa llega luego de muchos amaneceres y atardeceres.

Este trabajo doctoral lo dedico a mi esposo Marco y mis hijos Antonella y Marco. Ellos han sido los grandes aportantes de amor, paciencia y motivación en estos años de estudio.

Este esfuerzo significó menos tiempo para ustedes para leerles cuentos, sentirlos dormir en mi regazo o, simplemente, compartir momentos en familia. En sus sonrisas y sus miradas también veo mi realización personal y profesional. Ese es el alimento emocional que necesito para seguir.

"El Principito", obra de Antoine de Saint-Exupéry, dice que para "reflexionar y tomarse la vida de otra forma, hay que exigir a cada uno lo que cada uno puede hacer". Yo lo hice por ustedes, para que el legado con el que recuerden a su mamá sea que los retos, por más grandes y difíciles que parezcan se asumen con valor y se cumplen con honor.

AGRADECIMIENTOS

A mi familia: mis padres, hermanos, sobrinos, suegros y primos que me acompañaron en este viaje.

A mi otra familia, la que se elige, porque comparten la misma pasión por la defensa de los derechos en los entornos digitales: Daniela, Cristián, Galo, Johana, Matthew, Vivi e Ili.

A mis maestras y amigas: la que está en el cielo, y que decidió apenas nos conocimos, que mi derecho sería el de la protección de datos personales, Rosario Valpuesta. La que está en la tierra porque se empeña en ponerme retos cada vez más difíciles, Alexandra Vela.

A mi director, maestro y amigo, Francisco Oliva, por su guía y apoyo en este difícil proceso de investigar y escribir, por su paciencia y generosidad en el conocimiento.

A mis discípulos y alumnos que colaboraron en este proyecto.

TABLA DE CONTENIDO

CAPITULO II

RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES EN EL MODELO EUROPEO

CAPITULO III

ARMONIZACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES EN AMÉRICA LATINA A TRAVÉS DE INSTRUMENTOS INTERNACIONALES

CAPÍTULO IV

EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL CONTEXTO LATINOAMERICANO

CAPITULO V

CONTENIDO ESENCIAL DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN LATINOAMÉRICA

EPÍLOGO

CONTENIDOS ESENCIALES DE UNA LEY PROTECCIÓN DE DATOS PERSONALES PARA ECUADOR

INTRODUCCIÓN

La revolución digital que actualmente vivimos ha transformado radicalmente la forma en que los seres humanos se desenvuelven en distintas actividades, como en el área política, económica, social, cultural, educativa, familiar, personal, entre otras. En este nuevo contexto, en el que las personas se desarrollan ha sido necesario redefinir las condiciones y estrategias para lograr un adecuado impulso digital en contornos de globalización. Esto, ha hecho necesario empezar a reconocer el valor de los datos personales como el eje central para lograr una economía digital sana, en donde, es necesario contar con legislación orientada a promover el adecuado tratamiento de este tipo de información, con la finalidad de generar confianza en el ecosistema digital, a través de arquitecturas, diseños y plataformas que otorguen seguridad tecnológica, para que los individuos transiten protegidos en este nuevo espacio, y, de marcos regulatorios que fomenten el adecuado tratamiento de datos personales para dotar de seguridad jurídica a todas las acciones y decisiones que ejecutan en dicho entorno.

Es ahí en donde el ordenamiento jurídico como forma de organización de la sociedad toman la posta en el desarrollo de las relaciones que se efectúan en entornos digitales, motivo por el cual es menester el estudio de la norma y los derechos que se generan en entornos digitales y más aún aquellos que se traspolan de él, al campo de la realidad, tal es el caso del derecho a la protección de datos personales, tema central del presente trabajo doctoral.

En donde el objetivo fundamental de la presente tesis doctoral es el establecer el contenido esencial del derecho a la protección de datos personales en el Ecuador a la luz de los modelos europeo, norteamericano y latinoamericano; de tal manera que se realice un estudio de las diversas formas de concepción de este derecho y cómo aterriza en el ámbito ecuatoriano.

En el génesis del presente, se elaborará un análisis profundo alrededor de la normativa constitucional ecuatoriana que ha llevado al reconocimiento del derecho a la protección de datos personales en la Constitución de la República del Ecuador de 2008, vigente hasta la actualidad, en el cual se tomarán algunos de los criterios jurisprudenciales de los máximos órganos de justicia en el Ecuador, que han tratado de darle forma a la concepción del mencionado derecho, que llevaron al constituyente a plasmarlo en el texto de la norma suprema.

Parte fundamental de este análisis es el camino que ha transcurrido el desarrollo del derecho a la protección de datos personales desde una primera alusión en la inviolabilidad del domicilio hasta su reconocimiento pleno; pasando por diversos cambios y en específico de su definición a través de la garantía constitucional del *habeas data*, que previo al establecer el derecho a la protección de datos personales en el texto constitucional ya se presentaba como una garantía de varios derechos que fueron dando origen al mismo.

En la segunda parte del presente trabajo se realizará una investigación relacionada con el contenido esencial del derecho a la protección de datos personales en el modelo europeo de manera que se desglosen las características de este sistema de protección de datos personales considerados como el de mayor estándar. Para lo cual se ha explicado la paulatina configuración del derecho; así como su evolución a través del reconocimiento de la

autodeterminación informativa como parte esencial como marca diferenciadora a la luz de los criterios jurisprudenciales europeos.

Así mismo, se entrará a analizar la evolución y armonización de la protección de datos personales en Europa a través de la Declaraciones, Convenios y directivas que tratan sobre la materia y que le han ido dando contenido a este derecho, realizando un estudio desde las primeras iniciativas hasta la situación actual de los datos personales; así mismo se analizará la Protección de Datos Personales en la normativa europea, con un especial énfasis en el Reglamento General Europeo de Protección de Datos Personales.

Es necesario recalcar que a través del crecimiento exponencial de las tecnologías de la Información y Comunicación, los datos personales se han convertido en aquella materia prima primordial para el desarrollo de los ecosistemas digitales, motivo por el cual dentro de las relaciones comerciales que se llevan a cabo en estos entornos América Latina se ha visto en desventaja como región frente a Europa, razones que motivaron a que en el presente trabajo se dedique un espacio a cómo la normativa se ha ido armonizando al modelo Europeo.

Es así como, pese a la potencial influencia de la *privacy* en la región debido a los pronunciamientos de organismos internacionales en materia de protección de derechos, en Latinoamérica, el modelo Europeo ha sido aquel llamado a encontrarse en las diversas legislaciones de los Estados de América Latina, tal como se desarrolla en el tercer capítulo del presente documento

Parte de esta confluencia de sistemas de protección en América Latina es el establecimiento de un derecho garantía como es el *habeas data* como un intento de establecer un mecanismo de protección que garantice el efectivo goce del derecho a la protección de datos personales y que en el caso particular de muchos Estados Latinoamericanos incluyendo el Ecuador, viabiliza el ejercicio de otros derechos reconocidos en la Constitución y en instrumentos internacionales de derechos humanos.

En virtud de lo expuesto, se encuentra la necesidad de analizar legislaciones de 21 Estados latinoamericanos para estudiar las características de cada uno y así identificar las tendencias hacia los modelos de protección de la *privacy* o europeo; de tal manera que se pueda conseguir una revisión general del estado situacional de la protección de datos personales en América Latina y cómo la aplicación de estándares de protección europeos pueden coadyuvar para el efectivo desarrollo de este derecho en la región.

No obstante el análisis servirá de base para entrar al estudio del sistema ecuatoriano de protección de datos personales y cómo la carencia de una normativa específica en materia de protección de datos personales revela las dificultades del Estado no solo al nivel del aseguramiento de los derechos de los titulares sino a nivel económico, cultural y social, que decantará en el Proyecto de Ley Orgánica de Protección de Datos Personales presentado ante la Asamblea Nacional del Ecuador para su tratamiento legislativo.

Para la presente investigación se realizará un análisis exegético y dogmático sobre el contenido esencial del derecho a la protección de datos personales en el Ecuador a la luz de los modelos europeo, norteamericano y latinoamericano, con el fin de desarrollar el derecho a la autodeterminación informativa como parte de su contenido esencial, para ejercer la libertad informática, de decidir qué datos, con qué finalidades y bajo qué circunstancias los titulares entregarán sus datos a responsables del tratamiento de datos personales. Finalmente, se

desarrolló un grupo de investigación liderado por la autora lideró que tenía por objetivo recopilar, organizar, sistematizar y analizar la jurisprudencia ecuatoriana sobre *habeas data*. Este proceso contó con la participación de Daniela Macías Villarreal como coordinadora y de los estudiantes del curso de Derecho Informático, Der 903-2 del período académico 2015-1, que va desde septiembre de 2014 hasta febrero de 2015 de la Universidad de las Américas.

CAPÍTULO I

CONFIGURACIÓN CONSTITUCIONAL DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR

1. Introducción y planteamientos iniciales

Mediante un análisis histórico jurídico, dogmático, jurisprudencial, constitucional y legal, el primer capítulo de la presente tesis doctoral tiene como objetivo principal determinar la evolución y el marco normativo vigente del derecho a la protección de datos personales en el Ecuador.

En algunos ordenamientos jurídicos la intimidad es el antecedente inmediato y recurrente de este derecho, por lo que es necesario, identificar si en el caso ecuatoriano se ha desarrollado de la misma forma evolutiva; además, verificar los motivos por los cuales se logró su independencia y autonomía.

Resta aclarar, si el proceso de reconocimiento paulatino del derecho a la protección de datos personales en Ecuador, permite identificar su contenido esencial para su posterior comparación con los contenidos mínimos de los modelos europeo, norteamericano y latinoamericano.

El *habeas data*[1] es otro de los antecedentes inmediatos del derecho a la protección de datos personales, siendo fundamental y pertinente el estudio de su evolución, sobre todo en Latinoamérica, con la finalidad de identificar sus diferentes dimensiones, así como la de otras garantías que el Estado ecuatoriano está obligado a implementar para propender a la efectiva vigencia del derecho constitucional relativo a datos personales.

Inicialmente se lo consideraba como un derecho-garantía; en otras palabras, además de constituirse como un mecanismo de tutela jurisdiccional, contenía en sí mismo varios de los componentes propios del derecho a la protección de datos personales. Posteriormente, esta garantía constitucional irá decantándose para precisar su procedencia, dimensiones y ampliación, ya que, por su intermedio, también pueden ser cautelados otros derechos como la honra, la intimidad, la privacidad, el derecho a la propia imagen, a la propia voz, entre otros.

Para cumplir con este objetivo es indispensable examinar la primera Constitución que reconoció a la intimidad como derecho fundamental, la reforma constitucional que incluye al *habeas data* como garantía jurisdiccional, para posteriormente revisar la Constitución del 2008 que es aquella que recoge el derecho a la protección de datos personales.

Luego de esta exploración se pretende dibujar la línea evolutiva del derecho a la protección de los datos personales en Ecuador y esclarecer, no solo nuestra situación actual, sino reconocer cuáles son las necesidades latentes para que los niveles de vigencia normativa y protección sean los óptimos.

En consecuencia, la revisión cronológica que consta a continuación contendrá información normativa, doctrinal, jurisprudencial e incluso describirá algunas prácticas oficiales, con la

finalidad de que la mirada sea profunda y completa que permitirá desarrollar conclusiones, lo más apegadas a la realidad ecuatoriana.

2. Antecedentes del reconocimiento constitucional a la protección de datos en Ecuador desde 1830 al 2008

El objetivo fundamental de este título es determinar si la incorporación del derecho a la protección de datos personales en Ecuador atravesó por procesos evolutivos similares a los desarrollados en Europa o Estados Unidos; es decir, si la intimidad o la privacidad fueron y en qué nivel antecedentes inmediatos del derecho a la protección de datos personales. Para lograr resolver este cuestionamiento es indispensable realizar una revisión general de las dieciocho Constituciones ecuatorianas promulgadas, en busca de los elementos primigenios que esbocen la vigente comprensión del derecho a la protección de datos personales.

Al respecto, las primeras formas de reconocimiento constitucional de la existencia de una esfera privada de las personas se materializan en derechos como la inviolabilidad del domicilio y la inviolabilidad de la correspondencia. Si bien estos derechos se protegen por razones propias y suficientes, en especial relacionadas con el ejercicio de otros derechos fundamentales como la libertad de expresión, la libertad ideológica e incluso con garantías al debido proceso, por su naturaleza son derechos que garantizan también la intimidad y la privacidad. La doctrina ha considerado, tanto a la inviolabilidad del domicilio, como a la inviolabilidad de la correspondencia como instrumentales de los derechos de la personalidad, lo que no quiere decir que no sean autónomos, sino que, por el contrario, refuerzan el sistema de protección.[1]

Para una amplia y completa revisión histórica, normativa y constitucional ecuatoriana se estudiará, adicionalmente, a la honra como derecho conexo de la intimidad y de la protección de datos personales. Sin duda, la afectación mediante la manipulación negativa de datos personales o de la difusión de información íntima afecta directamente a la dignidad de la persona y a la proyección que tiene en el medio social.

Asimismo, se encontrarán referencias directas a la intimidad como derecho fundamental, al *habeas data* como garantía constitucional y, recientemente, a la protección de datos personales.

Una adecuada revisión constitucional exige un mapeo desde la Constitución de 1830 hasta la vigente. Una profundización de la investigación desde la Constitución de 1967 porque en ella se recoge por primera vez a la intimidad como derecho fundamental. En este sentido, se acudió al Archivo General de la Asamblea Nacional del Ecuador para obtener las actas de debate de las Constituciones de 1967, 1978 con sus respectivas reformas, 1998 y la vigente de 2008, con la finalidad de extraer información de los motivos sociales, culturales, políticos o académicos que motivaron la incorporación de los distintos textos constitucionales a ser analizados a continuación.[2]

[1] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional* (Barcelona: Atelier, 2012), 302-3.

[2] Las actas se encuentran digitalizadas pero no indexadas por lo que se ha tenido que leer una gran cantidad de información, no necesariamente pertinente, para extraer lo atinente a nuestro tema de estudio.

2.1 Evolución constitucional del Ecuador desde los albores de las República hasta nuestros días.

Para lograr una adecuada contextualización usaremos el estudio sobre periodización general de la historia ecuatoriana realizado por el historiador ecuatoriano Enrique Ayala Mora.[3] De tal manera que se revisarán únicamente dos épocas: la denominada de Independencia y Etapa Colombiana y, la segunda, llamada Época republicana.

Respecto de la primera, la historia constitucional ecuatoriana se remonta a 1812 cuando se reúne la primera Asamblea en la que se discute y aprueba la llamada Constitución quiteña, que fue resultado de la gesta emancipadora del 10 de agosto de 1809 y que rigió pocos meses, puesto que el gobierno español fue restaurado. Su contenido declarativo se considera un antecedente histórico más que normativo.

Asimismo, la independencia del Ecuador de 1822 permitió, junto con Colombia y Venezuela, conformar la Gran Colombia. De esta época, se dicta la Constitución de Cúcuta de 1821. También se la considera antecedente histórico porque se trata de otro Estado distinto al ecuatoriano. Finalmente, la de Bogotá de 1830 que no tuvo vigencia, ya que en ese mismo año se disolvió la Gran Colombia.

Este recuento constitucional empieza realmente con la Constitución de 1830, que es aquella que crea al Ecuador como Estado soberano e independiente de la colonia española y de las ideas unificadoras de la Gran Colombia. A este período histórico se le ha denominado Época republicana.

En Ecuador, desde su conformación como República, se han dictado veinte Constituciones[4, 5] incluida la vigente de 2008. Esta inestabilidad constitucional ha sido producto de varios

[3] E. AYALA MORA, *Historia, tiempo y conocimiento del pasado: estudio sobre periodización general de la historia ecuatoriana una interpretación interparadigmática* (Quito: Corporación Editora Nacional, 2014), 9.

[4] J. TOBAR DONOSO Y J. LARREA HOLGUÍN manifiestan: "Son veinte constituciones las dictadas en el Ecuador desde 1830 hasta el 2017: 1. Riobamba, 23 de septiembre de 1830 – Presidencia de Juan José Flores; 2. Ambato, 13 de agosto de 1835 - Presidencia de Vicente Rocafuerte; 3. Quito, 1 de abril de 1843 - Presidencia de Juan José Flores. 4. Cuenca, 8 de diciembre de 1845 - Presidencia de Vicente Ramón Roca; 5. Quito, 27 de febrero de 1851 - Presidencia de Diego Noboa; 6. Guayaquil, 6 de septiembre de 1852 - Presidencia de José María Urbina; 7. Quito, 10 de abril de 1861 - Presidencia de Gabriel García Moreno; 8. Quito, 11 de agosto de 1869 - Presidencia de Gabriel García Moreno; 9. Ambato, 6 de abril de 1878 - Presidencia de Ignacio de Veintimilla; 10 Quito, 13 de febrero de 1884 - Presidencia de José Plácido Caamaño; 11. Quito, 14 de enero de 1897 - Presidencia de Eloy Alfaro Delgado; 12. Quito, 22 de diciembre de 1906 - Presidencia de Eloy Alfaro Delgado; 13. Quito, 26 de marzo de 1929 - Presidencia de Isidro Ayora Cueva; 14. Quito, 2 de diciembre de 1938 - Presidencia de Aurelio Mosquera N. (no fue promulgada pero se la estudia por su contenido histórico); 15. Quito, 6 de marzo de 1945 - Presidencia de José María Velasco Ibarra; 16. Quito, 31 de diciembre de 1946 - Presidencia de José María Velasco Ibarra; 17. Quito, 25 de mayo de 1967 - Presidencia de Otto Arosemena G.; 18. Quito, 15 de enero de 1978 - Triunvirato "Militar; 19. Riobamba, 5 de junio de 1998 - Presidencia Interina de Fabián Alarcón; 20. Montecristi, 28 de septiembre de 2008 - Presidencia de Rafael Correa Delgado. No se cuenta con la Constitución emitida por la Junta Quiteña de 1812 O Constitución del Estado de Quito, los Estatutos de la Junta Patriótica de Guayaquil, la Constitución de Cuenca de 1822, las Constituciones de la Gran Colombia que tuvieron precaria vigencia en el territorio del actual Ecuador y la de 1938 que no entró en vigor. La mayoría ha sido dictadas por asambleas constituyentes; excepto dos, incluida la vigente, que fueron aprobadas por consulta popular". Ver JULIO TOBAR DONOSO Y JUAN LARREA HOLGUÍN, JUAN, *Derecho constitucional ecuatoriano* (Quito: Corporación de Estudios y Publicaciones, 1996), 88. ENRIQUE AYALA MORA, *Resumen de historia del Ecuador* (Quito: Corporación Editora Nacional, 1993), 58.

[5] Ibíd.

momentos políticos, sociales y económicos que han marcado la historia del Ecuador, así como de una tendencia generalizada a utilizar a la Carta Magna como plan de gobierno.

La periodización histórica del Ecuador puede ser directamente relacionada con los períodos de evolución constitucional del Ecuador; de tal forma que podemos dividirlos de la siguiente manera:

a) **Primer período republicano: Proyecto nacional criollo.** Que va desde la fundación de la República (1830-1850), la consolidación del Estado oligárquico terrateniente (1860-1875) hasta el auge y caída del Estado oligárquico terrateniente (1875-1895). Juristas ecuatorianos desde la perspectiva constitucional han denominado a esta etapa: *De formación del Estado ecuatoriano.*

   Forman parte de este período un total de diez Constituciones. Este bloque de Constituciones se organiza por períodos cronológicos basados en las máximas autoridades o en sus bases ideológicas. Período floreano: Constituciones de 1830, 1835 y 1843 (Carta de la esclavitud); período marcista: Constituciones de 1845, 1851 y 1852; período garciano: 1861 y 1869 (Carta Negra); período posgarciano: Constitución de 1878; período progresista: Constitución de 1884.[6]

   Inicia con la Constitución de 1830, en la que se crea, aunque tímidamente,[7] un Estado ecuatoriano soberano e independiente. Las ocho siguientes recogen, adaptan y desarrollan el denominado constitucionalismo clásico.[8] Mantienen como elemento común el sufragio indirecto y restringido por ciudadanía, edad, alfabetización e incluso por capacidad económica. La mayoría de los cambios normativos sufridos en estos cuerpos constitucionales se refieren a la forma de organización de los poderes del Estado.

b) **Segundo período republicano: Proyecto nacional mestizo.** Inicia con la Revolución Liberal (1895-1912), predominio plutocrático (1912-1925), la crisis, inestabilidad e irrupción de las masas (1925-1947) y una etapa de estabilidad (1948-1960). Por su parte, los juristas constitucionales consideran a esta etapa como de consolidación del Estado ecuatoriano.

   Un total de siete[9] Constituciones conforma esta etapa del constitucionalismo ecuatoriano, el cual empieza con el período liberal manifestado en las Constituciones

[6] Si bien el autor sostiene que son parte de este período de formación del Estado ecuatoriano las Constituciones del período liberal (Constituciones de 1897 y 1906), como estamos utilizando la periodización general de la historia ecuatoriana de Enrique Ayala Mora como referente organizativo, dichas constituciones pasan a conformar el siguiente período, lo que resulta mejor desde la perspectiva de los contenidos ideológicos de las Cartas Magnas que precisan un proyecto nacional mestizo. HERNÁN SALGADO PESANTES, *Lecciones de Derecho Constitucional* (Quito: Ediciones Legales S.A., 2012), 76.

[7] "Esta primera Constitución era rudimentaria y defectuosa en algunas cuestiones jurídico-políticas, y resultó un tímido intento por organizar un Estado soberano e independiente. Justamente su mayor error estuvo en declarar de modo unilateral que el Ecuador «se une y confedera con los demás Estados de Colombia para formar una sola nación con el nombre de República de Colombia» (artículo 2). De esto se deduce que el ordenamiento jurídico que se daba al nuevo Estado resultaba provisional, además de que se lo revestía con una aparente soberanía". Ibíd., 83.

[8] Ibíd., 76.

[9] Constituciones de 1897, 1906, 1929, 1938 (que no fue promulgada y por eso se considera jurídicamente inexistente) 1945, 1946, 1967, ibíd., 77.

de 1897 y 1906 que establecen la formación de un Estado de corte liberal.[10] Se divide en dos subperíodos: El primero representado con la Constitución de 1929, que refleja el constitucionalismo social de posguerra que reconoce los derechos sociales y económicos como el trabajo, la previsión social, acceso a servicios públicos, salud, educación, vivienda y familia; así como el recurso de hábeas corpus como garantía de libertad individual especialmente frente a la persecución política. Se reconoce a la mujer sus derechos políticos y al voto. Se modifica nuevamente la organización del poder estatal.

El segundo subperíodo contempla las Constituciones de 1945, 1946, 1967. Las tres primeras desarrollan una dimensión social en el ámbito de los derechos humanos, no solo al incluir en su texto varios de los derechos reconocidos en las Declaraciones y Convenciones Internacionales de Derechos Humanos, sino por establecer al Estado como su garante.

c) **Tercer período republicano: Proyecto nacional de la diversidad.** De la crisis al auge petrolero (1960-1979), del auge a la crisis y al neoliberalismo (1979-2000), y finalmente los últimos años (2000). A este período pertenecen las Constituciones de 1978 con sus cuatro reformas, la Constitución de 1998 y la vigente de 2008.

Antecedente inmediato y directo de la Constitución vigente es la Constitución de 1978, que pese a su contenido de reconocimiento de derechos sociales, conforme varios autores, tenía un corte liberal clásico.[11] Es la primera del nuevo período democrático ecuatoriano, con sus diez años de vigencia. Pese a las distintas reformas realizadas al texto constitucional, que motivaron por cuatro ocasiones su codificación[12] para mantener la coherencia de la norma, es la de mayor duración en la historia del Ecuador. Precisamente, se optó por un proceso de reformas y no de sustitución por cuanto se buscaba, mediante la normativa constitucional, estabilidad democrática y la mejora de la institucionalidad por medio de la paulatina depuración del contenido, sin tener que acudir a nuevas Constituyentes.

Las cuatro reformas fueron las siguientes: primera reforma, las de 1983 que entraron en vigencia el 10 de agosto de 1984; segunda reforma, las de fines de 1992 y cuya codificación se publicó el 5 de mayo de 1993; tercera reforma, la aprobada el 16 de enero de 1996, en el período del interinazgo del presidente Fabián Alarcón; cuarta reforma, la del 11 de agosto de 1998 mediante la Constituyente que desarrolló una reforma integral que modificaba casi en su totalidad la Constitución de 1978.[13]

La Constitución de 1998, por primera vez, define al Ecuador como Estado social de derecho; es decir, reconoce a la igualdad real por encima de la formal, contempla sujetos y derechos, individuales y colectivos. Consagra al catálogo de valores,

[10] Ibíd., 76.
[11] G. PISARELLO, *Un largo termidor: historia y crítica del constitucionalismo antidemocrático* (Quito: Corte Constitucional para el Período de Transición, 2011), 190.
[12] Primera Codificación de la Constitución Política de 1978, realizada en 1984 y publicada en el RO, No. 763 (12 de junio de 1984); Segunda Codificación de la Constitución Política de 1978, Ley No. 25, publicada en el RO, No. 183 (5 de mayo de 1993); Tercera Codificación de 1996, publicada en el RO, No. 969 (18 de junio de 1996); Cuarta codificación de la Constitución Política de 1978, realizada en 1997 y publicada en el RO, No. 2 (13 de febrero de 1997).
[13] La consulta popular de 1997 incluyó una pregunta relativa a la convocatoria a la Asamblea Constituyente que permitió elaborar la Constitución Política del Ecuador de 1998.

principios y derechos fundamentales como norma suprema, vinculante y de aplicación directa. Determina la existencia de garantías jurisdiccionales constitucionales e incluye a la interpretación extensiva para resolver, tanto las antinomias constitucionales como las legales.

La Constitución de 1998 no logró satisfacer las necesidades económicas y sociales de las personas y colectivos y "el empeño en mantener las políticas de ajuste financiero y económico desató una sostenida resistencia indígena y movimientos urbanos que cobró tres gobiernos: el de Abdalá Bucarán, en 1997; el de Jamil Mahuad, en el 2000 y el de Lucio Gutiérrez, en 2005. Este vendaval destituyente arrastró consigo a la constitución de Sangolquí, pactada en 1998 entre las fuerzas sociales constituyentes y los partidos tradicionales...".[14]

Algunos constitucionalistas entre los que destacan Ortiz Crespo[15], Montúfar[16] y Burbano de Lara[17] señalan que con la Constitución de 2008 aparece un nuevo período denominado garantismo. Al respecto se desarrollará su contenido a profundidad al contextualizarse la incorporación del derecho a la protección de datos personales. Por el momento, vale mencionar que esta etapa está representada por la definición del Ecuador como un Estado de derechos y justicia social, plurinacional y democrático, entre otras características. Se considera garantista por cuanto desarrolla un marco de principios, derechos y garantías a favor del respeto a la dignidad humana.

Esta breve descripción histórica y jurídica de carácter constitucional nos permitirá enmarcar temporalmente y comprender la configuración de los distintos derechos precedentes próximos del derecho a la protección de datos, que se analizarán a continuación.

2.2 Inviolabilidad de domicilio (1830)

La inviolabilidad de domicilio, reconocida en las Constituciones ecuatorianas de 1830 y 1946, no podía, ni remotamente, asociarse al derecho a la intimidad personal o familiar, menos aún proteger datos personales, físicos o virtuales. Sin embargo, es referente inmediato y directo, ya que el primer reducto de espacio íntimo o privado es el domicilio de la persona.

En la teoría general de los derechos se señala a la libertad negativa como aquella que impide al Estado y a los particulares actuar en perturbación de los derechos de otros. En este sentido, la inviolabilidad de domicilio involucra un deber de abstención en pro de garantizar la libertad del ser humano. Criterio que coincide con la dimensión negativa con la que actualmente se aborda el derecho a la intimidad.[18]

La primera Constitución de 1830, expedida en Riobamba por el Congreso Constituyente el 11 de septiembre del mismo año establece: "elementalmente, los derechos humanos y garantizar su respeto. De esa enumeración y garantías incipientes, se llegará progresivamente a mejores

[14] E. AYALA MORA, *Resumen de historia del Ecuador*, 192.
[15] Q, ORTIZ CRESPO, *Estado constitucional de derechos: informe sobre derechos humanos* (Ecuador: Universidad Andina Simón Bolívar, 2010), 46.
[16] C. MONTÚFAR, *Plenos poderes y transformación constitucional* (Ecuador: Abya-Yala, 2008), 370.
[17] F. BURBANO DE LARA, *Transiciones y rupturas: El Ecuador en la segunda mitad del siglo XX* (Ecuador: FLACSO, 2010), 133
[18] I. BERLÍN, *Cuatro ensayos sobre la libertad* (Madrid: Alianza, 1998), 229.

formulaciones y más eficaces sistemas de protección: cada Constitución prácticamente representa un paso adelante en este importante aspecto jurídico".[19]

Al respecto, la primera Carta Magna ecuatoriana recoge como garantía del ciudadano la siguiente: "Artículo 65.- La casa de un ciudadano es un asilo inviolable; por tanto no puede ser allanada sino en los casos precisos, y con los requisitos prevenidos por la ley". Esta redacción recoge la visión de que la propiedad (la casa) es el *asilo inviolable* como una forma de proteger al ciudadano de las injerencias arbitrarias de los poderes públicos. Se permite el allanamiento, únicamente en los casos previamente establecidos en la ley, generalmente asociados al cometimiento de una infracción o de una emergencia: incendio, inundación, entre otras, aunque para este último no se habla históricamente de autorización de la ley, sino que se supone razonablemente el permiso del dueño o habitador.[20] Lejos estaba el pensar proteger el derecho al domicilio de una persona por considerarlo un espacio obvio de privacidad e intimidad. La condición de ciudadano se garantizaba solo a aquellos que tenían condiciones económicas que garanticen su independencia como electores.[21]

En la misma Constitución consta lo siguiente: "Artículo 63.- Los militares no podrán ser alojados en casas particulares, o de comunidad sin avenimiento de los dueños. Se prepararán conforme a las leyes, cuarteles y alojamientos para oficiales y tropa que vayan en servicio en tiempo de paz o de guerra. Queda proscrita la ley marcial". De esta forma se evitaban los abusos por parte de las fuerzas militares y se configuraba entonces una norma que completaba el respeto por la morada precautelando la conflictividad, marcada por las pugnas políticas, de aquel entonces.[22]

En la Constitución expedida en Ambato por la Convención el 30 de julio de 1835, nuevamente, en el título De las Garantías, incluye un texto similar a su predecesora: "Artículo 105.- La casa de toda persona que habite el territorio ecuatoriano, es un asilo inviolable, y solo puede ser allanada por un motivo especial determinado por la ley, y en virtud de orden de autoridad competente". Como vemos, una de las variantes es la de eliminar la condición de ciudadano que constaba en el texto anterior, para señalar que son titulares de este derecho todas las personas que habiten el territorio; es decir, se incluye en el ámbito de protección tanto a ecuatorianos que no son ciudadanos, así como a extranjeros. La condición de ciudadanos subsiste únicamente para efectos de participación política no para la garantía de este derecho.

Adicionalmente, se establece la excepción del allanamiento no solo cuando lo ha facultado la ley, como rezaba el texto anterior, sino que además incluye a la orden de autoridad competente. Es decir, un acto sustitutivo del consentimiento del titular que valora los casos en los que se justifica legalmente la intromisión de ajenos en la casa de un individuo, sin la autorización del juez, no es posible el allanamiento ya sea para revisar sus pertenencias o para detenerlo por el cometimiento de un delito, por ejemplo.

Al igual que la anterior Constitución, ante la realidad histórica, consta la siguiente norma que pretende salvaguardar la propiedad privada y la inviolabilidad del domicilio por parte de las fuerzas militares: *"*Artículo 102.- Los militares no podrán ser alojados en casa de los demás

[19] J. LARREA HOLGUÍN, *Derecho constitucional ecuatoriano* (Quito: Corporación de Estudios y Publicaciones, 2000), 5.
[20] Ibíd., 229.
[21] Ibíd., 20.
[22] E. AYALA MORA, *Historia, tiempo y conocimiento del pasado*, 95 y s.

ecuatorianos sin consentimiento de los dueños; ni hacer requisiciones, ni exigir clase alguna de auxilios, sino por medio de las autoridades civiles".

Posteriormente, la Constitución Política de 1843, generalmente conocida como la Carta de la Esclavitud, expedida en Quito por la Convención Nacional, el 31 de marzo de 1843 nuevamente consagra el derecho a la inviolabilidad de la casa en iguales condiciones que su antecesora. El texto expresamente señala: "Artículo 99.- La casa de toda persona que habite el territorio ecuatoriano, es un asilo inviolable, y solamente puede ser allanada por un motivo especial determinado por la ley, y en virtud de orden de la autoridad competente".

Norma similar en contenido a sus predecesoras consta en la Constitución de 1843 respecto de la prohibición de que los militares puedan ingresar a un domicilio. Esta norma contiene el principio de reserva legal que hasta entonces no había sido incluido. La norma señala "Artículo 98.- Los militares no podrán ser alojados en casa de los demás ecuatorianos sin consentimiento de sus dueños; ni hacer requisiciones, ni exigir clase alguna de auxilios, sino por medio de las autoridades civiles, y en la forma, y casos que determine la ley".

Para 1845 cuando la Convención dicta en Cuenca la nueva Constitución consta una norma con texto idéntico en el que solamente se sustituye el término *casa* por el de *morada* sin que el resto del contenido del derecho sufra modificación alguna. La norma en cuestión textualmente menciona: "Artículo 127.- La morada de toda persona que habite el territorio ecuatoriano, es un asilo inviolable, y sólo puede ser allanada por motivo especial, determinado por la ley, y en virtud de orden de autoridad competente".

Asimismo, el artículo 129 señala que "nadie puede ser obligado en tiempo alguno a dar alojamiento a uno o más militares". Esta norma mantiene el mismo espíritu que sus antecesoras, pero se afianza en la aseveración de que no existe *tiempo alguno* que viabilice dar alojamiento a militares, o como en versiones anteriores que justifique requisiciones o prestación de auxilios. En el mismo sentido, consta una disposición idéntica en el artículo 119 de la Constitución de 1851 y el artículo 128 de la Constitución de 1852.

En la Constitución Política de 1851, expedida en Quito por la Convención, se unifica en una misma norma el derecho a la inviolabilidad de la morada y la inviolabilidad de la correspondencia. La norma literalmente dice: "Artículo 112.- No podrá ser allanada la casa de ningún ecuatoriano, ni su correspondencia o papeles interceptados o registrados sino por la autoridad, en los casos y con las formalidades prescritas por la ley".

Pese a que las anteriores normas establecían la garantía de este derecho a ecuatorianos y extranjeros, esta norma vuelve a limitar la protección únicamente a los ecuatorianos. Deja de usarse la fórmula *asilo inviolable* que tiene una clara connotación al refugio o resguardo que simboliza la casa de una persona y se la sustituye por la negación abierta *no podrá ser allanada la casa*. Nuevamente la norma señala que existen excepciones legales que permiten el allanamiento y que deberán estar debidamente autorizadas, pero omite la palabra competente. Esta omisión permite que no solo autoridades jurisdiccionales, sino otros poderes del Estado puedan dictar una orden de allanamiento; sin duda, esta omisión marca un nivel de desprotección pues la limitación a derechos fundamentales no puede provenir de cualquier nivel de autoridad, sino únicamente de aquella de carácter jurisdiccional. Esta Constitución permite facultades extraordinarias como el derecho a confinar, así como

mantiene *"*la innovación hecha por Constitución anterior, según la cual el Ejecutivo podía disponer en caso de peligro interior de los caudales afectos a objetos especiales".[23]

En la Constitución de 1852 dictada en Guayaquil por la Asamblea Nacional el 30 de agosto, en el artículo 126, nuevamente se separan las normas sobre inviolabilidad de domicilio y de correspondencia, y se incluye las referencias al *asilo inviolable* y a la autoridad *competente* conforme el contenido de la Constitución de 1845. Sin embargo, pese a la exigencia de que la orden provenga de autoridad competente; no se refuerza la garantía, porque la norma no expresa quién ha de ser competente.[24]

Tanto en la Constitución del año 1861, expedida en Quito por la Convención Nacional, en su artículo 120, como en la Constitución conocida como Carta Negra, expedida en Quito por la Convención Nacional el 9 de junio de 1869, consta texto idéntico, cuyo contenido relativo a esta última Constitución citada se trascribe a continuación: "Artículo 105.- La morada de toda persona que habite en el territorio ecuatoriano es un asilo inviolable, y sólo puede ser allanada por motivo especial que determine la ley y por orden de la autoridad competente". Ahora bien, esta norma se debilita porque ante la declaratoria de estado de sitio, el Presidente de la República tiene la facultad extraordinaria de ordenar allanamientos y registro de domicilio de personas sospechosa (artículo 61, numeral 1).[25]

Asimismo, tanto en el artículo 121 de la Constitución de 1861 como en el artículo 106 de la Constitución de 1869, la norma relativa al alojamiento de militares pierde fuerza. Si bien, las anteriores no permitían excepción alguna para que se faculte el alojamiento privado de militares, en las citadas Constituciones se faculta excepciones: de ocupar colegios y casas en casos extremos, así como la obligatoriedad de pagar alquiler si se produce un alojamiento en bienes que no pertenecen al Estado.

Para 1878, la Asamblea Nacional expide en Ambato una nueva Constitución Política que modifica la organización estructural del cuerpo normativo. "Esta Constitución inició la costumbre de colocar el título de Garantías entre los primeros, al revés de lo que había ocurrido hasta entonces (…) El artículo 16, propuesto por Don Pedro Carbo, consignó expresamente que «la Nación ecuatoriana reconoce los derechos del hombre como base y objeto de las instituciones sociales». La enumeración de las garantías fue hecha de manera más técnica y ordenada que las anteriores; y comprendió mayor número de derechos individuales…".[26] Se reconoce a los derechos fundamentales como la base y el objeto de las instituciones sociales (artículo 16), y en consecuencia se consagra la lista de derechos fundamentales a los que está obligada la nación.

Acerca del derecho a la inviolabilidad del domicilio, se sustituye el término *morada* que se había utilizado hasta entonces en los textos constitucionales por la palabra *hogar*, término que no suele utilizarse en el ámbito jurídico por sus connotaciones sociales y con el que se sustituye la frase *asilo inviolable* anteriormente usada. Conforme la doctrina de la intimidad, *hogar* es un término asociado directamente con los ámbitos en que se desarrolla la vida privada de las personas, sin embargo no existe evidencia de que haya sido usada con ese enfoque. El mencionado artículo señala: "Artículo 17.- La Nación garantiza a los

[23] J. TOBAR DONOSO Y J. LARREA HOLGUÍN, *Derecho Constitucional ecuatoriano*, 33-4.
[24] R. BORJA Y BORJA, *Derecho Constitucional Ecuatoriano*, vol. I, (1979), 195.
[25] Ibíd.
[26] J. TOBAR DONOSO Y J. LARREA HOLGUÍN, *Derecho constitucional ecuatoriano*, 47.

ecuatorianos: 4. El hogar, que no puede ser allanado sino por un motivo especial determinado por la ley, y por orden de autoridad competente...".

En la Constitución Política de 1884, expedida en Quito por la Asamblea Nacional, la norma textualmente expone: "Artículo 29.- La morada de toda persona es inviolable; no se allanará sino por motivo especial, que la Ley determine, y por orden de autoridad competente"; es decir, se vuelve a utilizar el término *morada* en lugar de *hogar* y además se elimina el término *asilo*. Texto idéntico consta en el artículo 20 de la Constitución Política de 1897, expedida en Quito por la Asamblea Nacional el 12 de enero. Ambas versiones son similares al contenido planteado en la versión de 1869. Adicionalmente, tanto en la Constitución de 1884 como en la Constitución de 1897 desaparece la norma que establecía que la nación ecuatoriana reconoce los derechos del hombre como la base y el objeto de las instituciones sociales, que constaba en la versión de 1878.

En el segundo período histórico de la época republicana, denominado Proyecto nacional mestizo, en el que consta la Constitución Política de 1906, expedida en Quito por la Asamblea Nacional y ordenada su publicación el 23 de diciembre, el texto varía en su ubicación en la estructura del texto constitucional, pues pasa a ser una de las garantías individuales que el Estado garantiza a los ecuatorianos: "De las garantías individuales y políticas. Artículo 26.- El Estado garantiza a los ecuatorianos: [...] 8. La inviolabilidad del domicilio; nadie puede penetrar en él, sin manifestar previamente orden por escrito de autoridad competente, y sólo en los casos determinados por la ley...". Esta Constitución, por sus propuestas innovadoras, generó seis años de conflictos bélicos internos. Incluyó por primera vez entre las garantías constitucionales, algunos derechos sociales relacionados principalmente con los derechos del trabajador y campesino, sus condiciones de salubridad, entre otros.

Adicionalmente, comienza a utilizarse el término *domicilio* que incluye no solo la morada o casa, sino que de conformidad con la doctrina civil ecuatoriana se incluye en el término al domicilio político[27] y el domicilio civil;[28] este último atado no solamente al hogar familiar o conyugal sino al negocio, lugar del ejercicio de la profesión u oficio, entre otros.[29] Desde la perspectiva de la intimidad, también se justifica el uso de este término; "de acuerdo con la jurisprudencia constitucional española «existe un nexo de unión indisoluble» entre la inviolabilidad del domicilio y el derecho a la intimidad, nexo que «obliga a mantener, por lo menos prima facie, un concepto constitucional de domicilio de mayor amplitud que el concepto jurídico privado o jurídico administrativo»" (STC 22/1984, FJ 2.°).[30]

En la Constitución Política de 1929, expedida en Quito por la Asamblea Nacional, en el Título XIII de las Garantías Fundamentales se señala los siguientes derechos: "Artículo 151.- La Constitución garantiza a los habitantes del Ecuador, principalmente, los siguientes

[27] ASAMBLEA NACIONAL DEL ECUADOR, [Código Civil Codificado, en ROS, No. 46 (24 de junio de 2005), Última modificación: 08 de julio de 2019]. ‹http://www.asambleanacional.gob.ec/es/leyes-aprobadas›. Consulta: 18 de febrero de 2018: "Artículo 46.- El domicilio político es relativo al territorio del Estado en general. El que lo tiene o adquiere, es o se hace miembro de la sociedad ecuatoriana, aunque conserve la calidad de extranjero. La constitución y efectos del domicilio político pertenecen al Derecho Internacional".

[28] Ibíd.: "Artículo 47.- El domicilio civil es relativo a una parte determinada del territorio del Estado".

[29] Ibíd.: "Artículo 49.- No se presume el ánimo de permanecer, ni se adquiere consiguientemente domicilio civil en un lugar, por el solo hecho de habitar en él un individuo, por algún tiempo, casa propia o ajena, si tiene en otra parte su hogar doméstico, o por otras circunstancias aparece que la residencia es accidental, como la del viajero, o la del que ejerce una comisión temporal, o la del que se ocupa en algún tráfico ambulante".

[30] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 303.

derechos: [...] 10. La inviolabilidad del domicilio. Nadie puede penetrar en domicilio ajeno sin consentimiento de su dueño o morador, o mediante orden escrita de autoridad competente y en la forma que determinen las leyes. Exceptúese el caso de auxilio a las víctimas de un delito o desastre...". Del texto se verifican varias precisiones que extrañan al contenido del artículo, relativas al consentimiento en el ingreso al domicilio y la excepción de auxilio de víctimas. Además, no garantizan propiamente el domicilio, pues no se determina quién ha de calificar a un acto o acontecimiento de delito o desastre.[31]

En la Constitución Política, expedida en Quito por la Asamblea Nacional Constituyente el 5 de marzo de 1945, en un texto casi idéntico al anterior se retira la precisión de ingreso al domicilio para el ingreso de víctimas de domicilio y desastre. El texto dice: "Artículo 141.- El Estado garantiza: [...] 8. La inviolabilidad del domicilio. Nadie puede entrar en domicilio ajeno sin consentimiento de su morador o sin orden de autoridad competente, expedida en la forma y en los casos que determine la ley...".

En la Constitución Política de 1946, en el título denominado Garantías individuales comunes aparece, el siguiente texto muy similar al anterior en contenido: "Artículo 187.- El Estado garantiza a los habitantes del Ecuador: [...] 6. La inviolabilidad del domicilio: nadie puede penetrar en el contra la voluntad de su dueño, a menos de presentar orden firmada por autoridad competente; y, sin esa orden, solo en los casos expresamente determinados por la ley...".

El primer antecedente de los derechos, deberes y garantías que recoge la Constitución de 1967 es la Constitución de 1945, considerada por los historiadores como progresista.[32] Aunque los principales derechos de contenido social y económico ya fueron recogidos en la Constitución de 1929, como señala Hernán Salgado Pesantez, en su obra *Lecciones de Derecho Constitucional*, quien menciona:

> "El desarrollo de los derechos humanos ha creado mayor conciencia en los pueblos para exigir su aplicación Lo cual ha sido una constante positiva en los países latinoamericanos una vez superados los últimos vestigios de las dictaduras. También el constitucionalismo ecuatoriano recogió esta tendencia y, como se sabe, lo estableció a partir de la Carta Política de 1929, la cual introdujo el denominado constitucionalismo social e incluso reconoció los derechos políticos de la mujer".[33]

Es parte del tercer período histórico republicano, denominado Proyecto nacional de la diversidad la Constitución de 1967, en la que aparecen varios textos que desarrollan los derechos humanos. Sin duda, esta declaración es reflejo inmediato y directo de las corrientes internacionales que propendían a la incorporación de la Declaración Universal de los Derechos Humanos en las normas internas de cada país. Así, el artículo 23 de la Constitución de 1967, expedida en Quito por la Asamblea Nacional Constituyente y publicada en el R.O. No. 133 de 25 de mayo de 1967, realiza una expresa mención respecto de la obligación del Estado de protegerlos: "Derechos humanos. El Estado reconoce, garantiza y promueve los derechos del hombre, como individuo y como miembro de la familia y demás sociedades que

[31] R. BORJA Y BORJA, *Derecho constitucional ecuatoriano*, 195.
[32] E. AYALA MORA, *Resumen de historia del Ecuador*, 97. "La llamada Gloriosa del 28 de mayo de 1944 fue un movimiento protagonizado por las masas populares que esperaban cambios radicales. Velasco manifestó en un principio ciertas inclinaciones a la izquierda, pero estas se desvanecieron cuando rompió la Constitución de 1945, preparada por una asamblea predominantemente progresista".
[33] H. SALGADO PESANTES, *Lecciones de Derecho Constitucional*, 61.

favorezcan el desarrollo de su personalidad. La ley protegerá la libertad y más derechos de la persona contra los abusos del Poder Público y de los particulares".

Esta norma fue debatida en la sesión de 10 de enero de 1967 en la Comisión de Constitución en la que participaron Andrés F. Córdova, Jorge Crespo Toral, Carlos Arízaga Vega, Julio César Trujillo, Carlos Cueva Tamariz, Alejandro Aguilar Ruilova y Rodrigo Suárez Morales. Entre las principales aportaciones en el debate consta la siguiente reflexión: "El H. Julio César Trujillo propone que en el artículo 21 mencionado, después de la palabra Estado se añada los términos «reconoce y promueve», puesto que el Estado no solo ha de garantizar, sino que ha de reconocer los derechos inherentes a la persona y anteriores a él, así como ha de promover esos derechos removiendo los obstáculos que impiden el pleno desarrollo del hombre".[34] Esta afirmación señala el deber del Estado no solo de reconocer, sino de promover los derechos, lo que sin duda se presenta como un avance para las Constituciones ecuatorianas. Por su parte, Crespo Toral sostiene que no es necesaria la mención expresa del segundo inciso del artículo 23 sobre la protección de los derechos frente al poder público. Sin embargo, nuevamente Julio César Trujillo señala que en "el primer inciso se halla el reconocimiento de la garantía y promoción de los derechos del hombre en general y mientras que en el segundo si bien incluye el concepto del primero se habla de la garantía de la ley frente al abuso del Poder Público y de los particulares".[35] Es decir, el Estado no solo debe ser garante de los derechos, sino que además se reconoce al Estado como uno de los transgresores de derechos por lo que la ley tiene como función ser el límite al poder estatal e incluso de los propios particulares.

La Constitución de 1967 recoge la mayoría de los derechos que manejamos actualmente en el vigente texto constitucional. Respecto del derecho a la inviolabilidad del domicilio, en el Capítulo II aparece el título De los Derechos de la Persona que dice: "Artículo 28.- Derechos garantizados.- Sin perjuicio de otros derechos que se deriven de la naturaleza de la persona, el Estado le garantiza: [...] 9. La inviolabilidad del domicilio: nadie puede entrar en habitación de otro sin su consentimiento o sin orden firmada por autoridad competente; sin tal orden, solo en los casos expresamente determinados por la ley". De este texto, similar a sus antecesores, destaca la inclusión de la reserva legal, es decir que los casos de excepción al derecho a la inviolabilidad del domicilio deben constar expresamente determinados en la ley.

En los debates de la Comisión de la Constitución se discutió la necesidad de que la orden que permite el allanamiento se encuentre firmada. El H. Villacrés argumentó "porque en la práctica se ve cuando hay violación de domicilio que se invoca tener orden de autoridad superior, pero después no hay cómo establecer responsabilidades".[36] Esta afirmación evidencia una de las transgresiones al debido proceso que se producían en esta época, lo que motivó la inclusión en la Constitución de la frase "orden firmada por autoridad competente".

Respecto de la Constitución de 1978, esta se divide en tres partes: la primera se refiere a los derechos, deberes, además incluye entre las finalidades del Estado la tutela de derechos fundamentales del hombre. La Constitución de 1978, aprobada en Referéndum del 15 de enero de 1978 y publicada en el R.O. No. 800, de 27 de marzo de 1979, en su versión original señala: "Título II De Los Derechos, Deberes y Garantías. Sección I. De los derechos de la Persona. Artículo 19.- Toda persona goza de las siguientes garantías: [...] 6. La inviolabilidad del domicilio. Nadie puede penetrar en él ni realizar inspecciones o registros, sin la

[34] COMISIÓN DE LA CONSTITUCIÓN DE ECUADOR DE 1967, [Acta No. 152], 4.
[35] Ibíd.
[36] Ibíd., [Acta No. 155], 1.

autorización de la persona que en él habita o por orden judicial, en los casos y forma que establece la ley...".

En la Primera Codificación de la Constitución Política de 1978, realizada en 1984 y publicada en el R.O. No. 763, de 12 de junio de 1984, aparece el siguiente texto: "Artículo 19.- Sin perjuicio de otros derechos necesarios para el pleno desenvolvimiento moral y material que se deriva de la naturaleza de la persona, el Estado le garantiza: [...] 7. La inviolabilidad de domicilio. Nadie puede penetrar en él ni realizar inspecciones o registros, sin la autorización de la persona que en él habita o por orden judicial, en los casos y forma que establece la ley; [...]". Si bien el contenido íntegro del ahora numeral 7 no se modifica, sí lo hace en la parte general del artículo 19. En dicho apartado, ya no se habla de garantías sino de derechos necesarios para el pleno desenvolvimiento de la persona y que el Estado garantiza.

Durante muchos años en Ecuador se asumió el concepto *garantía* como sinónimo de derecho, lo que es superado en esta codificación, pues sin duda se efectiviza un derecho mediante las garantías constitucionales que son instrumentos de protección. La referencia a otros derechos necesarios para el pleno desenvolvimiento moral y material, que se deriva de la naturaleza de la persona, "señala el verdadero fundamento de los derechos humanos: la naturaleza del hombre. Equivalen a las palabras de la Constitución a un reconocimiento del Derecho natural, al que se sujeta el Estado, y de que debe garantizar en toda su amplitud, aun cuando no exista una expresa declaración constitucional".[37]

En la Segunda Codificación de la Constitución Política de 1978, Ley No. 25, publicada RO, No. 183 (5 de mayo de 1993), consta el artículo 19, numeral 7, con un texto idéntico al anterior. La Constitución Política de 1978, en su Tercera Codificación de 1996, publicada en el RO, No. 969 (8 de junio de 1996), Título II, "De los derechos, deberes y garantías", Sección I, "De los derechos de las personas", Principios generales, señala en el ahora numeral 8 del artículo 22, cuyo texto es idéntico al anterior. En el mismo sentido lo hace la Cuarta codificación de la Constitución Política de 1978, realizada en 1997 y publicada en el RO, No. 2 (13 de febrero de 1997).

Sobre la Constitución Política de 1998, en el Título III, "De los derechos, garantías y deberes", Capítulo 2, "De los derechos civiles", en el siguiente texto se señala: "Artículo 23.- Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: [...] 12. La inviolabilidad de domicilio. Nadie podrá ingresar en él ni realizar inspecciones o registros sin la autorización de la persona que lo habita o sin orden judicial, en los casos y forma que establece la ley".

Finalmente, en la Constitución de la República del Ecuador de 2008, aprobado por la Asamblea Nacional de Montecristi y publicado en el RO, 449 (20 de octubre de 2008), en el Título II, "Derechos", Capítulo segundo, "Derechos del buen vivir", Capítulo sexto, "Derechos de libertad", consta el siguiente texto: "Artículo 66.- Se reconoce y garantizará a las personas: [...] 22. El derecho a la inviolabilidad de domicilio. No se podrá ingresar en el domicilio de una persona, ni realizar inspecciones o registros sin su autorización o sin orden judicial, salvo delito flagrante, en los casos y forma que establezca la ley".

[37] J. TOBAR DONOSO Y J. LARREA HOLGUÍN, *Derecho constitucional ecuatoriano*, 189.

Por primera vez se determina como excepción el caso del delito flagrante que permite la persecución del delito, en especial de aquellos relativos a violencia intrafamiliar.

En el primer debate se realizó la siguiente intervención: "No debemos dejar a la ley la limitación, ni de la libertad de circulación, ni la libertad de residencia sino que se debe poner expresamente en la misma carta Política en qué circunstancias se va a limitar la libertad de tránsito y la libertad de residencia".[38] Es decir, se consideraba que la reserva legal era insuficiente para garantizar este derecho y se pretendía que las limitaciones constaran expresamente en el texto constitucional. Esto demuestra la importancia para los asambleístas que este derecho tiene en el ejercicio de las libertades individuales. Esta posición, sin embargo, no tuvo eco y permaneció la reserva legal como forma de limitar este derecho.

En esa Constitución aparece la constancia expresa de los derechos que se limitan en un estado de excepción conforme el "Artículo 165.- Durante el estado de excepción la Presidenta o Presidente de la República únicamente podrá suspender o limitar el ejercicio del derecho a la inviolabilidad de domicilio, inviolabilidad de correspondencia, libertad de tránsito, libertad de asociación y reunión, y libertad de información, en los términos que señala la Constitución".[39] Nuevamente, la Constitución de 2008, al realizar un enlistamiento de los derechos que podrán ser suspendidos en un estado de excepción, hace expresa alusión a la inviolabilidad del domicilio; sin duda mediante esta limitación se puede lograr el control de la situación y de la población que permita afrontar ya sea una agresión, un conflicto armado, internacional o interno, conmoción interna, calamidad pública o desastre natural.

Del análisis realizado podemos evidenciar la comprensión paulatina del derecho a la inviolabilidad del domicilio, ya que las Constituciones que pertenecen a la primera época republicana amparaban este derecho desde la protección a la *casa como asilo inviolable* o de la *morada*; esto debido a que dicho período "estaba dominado por las élites latifundistas que triunfaron en el guerra de Independencia. Con este marco debemos estudiar la vida del pueblo, de la sociedad, bajo el predominio del Estado Oligárquico Terrateniente y el intento de constitución inicial de un proyecto nacional criollo".[40]

Es decir, los criollos como dueños de la tierra eran aquellos que tenían los medios económicos para ser reconocidos como ciudadanos de conformidad con las Constituciones de la época. Poseían propiedades y, por ende, a quien estaba direccionado en la práctica este derecho; toda vez que, habían subordinado a su poder a los artesanos, pequeños propietarios e indígenas, anotándose que la ocupación del territorio ecuatoriano era parcial pues cubría los valles interandinos y las riberas de los ríos tributarios del Guayas.[41]

Posteriormente, en la segunda etapa, llamada proyecto nacional mestizo, que se manifiesta abiertamente con la Constitución liberal de 1906 se usa por primera vez el término *domicilio* que incluye la morada o casa y que se utiliza unívocamente en todas las Constituciones que se dictan posteriormente, puesto que el domicilio no solo comprende la propiedad de la casa, sino un concepto más amplio que incluye el lugar de vivienda, el trabajo, el negocio, el almacén, entre otros. Todos ellos, espacios donde las personas desarrollan de forma ordinaria sus interacciones laborales, comerciales, personales y familiares y deben ser protegidas de invasiones a la privacidad e intimidad.

[38] ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 50], 172.
[39] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR [2008].
[40] E. AYALA MORA, *Historia, tiempo y conocimiento*, 114.
[41] Ibíd.

En ese período llama la atención que este derecho es considerado como una de las garantías individuales que el Estado garantiza a los ecuatorianos, con lo cual también se visibiliza desde esta época la importancia de los derechos para la sociedad ecuatoriana. Este es un elemento común que se manifiesta en las tres etapas de la historia del Ecuador; también es de considerar que el derecho a la inviolabilidad del domicilio se justifica en la necesidad de proteger a los ciudadanos de las posibles injerencias y persecuciones políticas. En realidad era un derecho garante de la libertad en sus distintas manifestaciones: ideológica, religiosa, de expresión. Esto se evidencia en las varias normas que señalaban la prohibición de las Fuerzas Armadas de ingresar, permanecer en el domicilio de los ciudadanos o de incautar sus bienes; asimismo, en la continua inclusión, eliminación o sustitución de las excepciones que permitían ingresar al domicilio como autorizaciones expresas de sus titulares, o por graves catástrofes, o por la comisión de delitos que además se especificaba podían ser de carácter político.

En las Constituciones del tercer período histórico, del proyecto nacional de la diversidad, nuevamente se evidencia la relación particular de este derecho con el ejercicio de las libertades, en especial la política y la ideológica. Tanto en los debates como en los contenidos constitucionales aprobados consta que solo una autoridad judicial puede autorizar allanamientos, ya que las autoridades administrativas o dependientes del Ejecutivo pueden convertirse en ejecutores de latentes persecuciones políticas.

Llama la atención en la mencionada Constitución que, en caso de delito flagrante se pueda producir la persecución del delito, en especial de aquellos relativos a violencia intrafamiliar; es decir, la privacidad nuevamente se manifiesta como un elemento a ser protegido. En consecuencia, es indispensable contar con una autorización judicial debidamente motivada que faculte el ingreso al domicilio de una persona. La ley determinará los requisitos, restricciones y condiciones que el juez valorará en cada caso concreto y que permitirán un dictamen debidamente motivado.

De la breve descripción normativa de las Constituciones ecuatorianas y de su encuadre histórico, podemos concluir que el derecho a la inviolabilidad del domicilio es una de las primeras formas de compresión de la esfera privada de las personas; y por lo tanto, una aproximación a la protección de lo privado, con un especial enfoque respecto de las libertades políticas.

La realidad ecuatoriana marca la protección constitucional del ejercicio de las libertades individuales, por medio de todos sus derechos en conjunto, entre los cuales, aun sin concebirse como tal, la privacidad forma parte del sistema mediante otras figuras como la inviolabilidad del domicilio, porque tanto de forma individual como en conjunto propenden al libre desarrollo de la personalidad y a la garantía del respeto a la dignidad humana.

2.3 Inviolabilidad de correspondencia (1835)

La finalidad fundamental de la inviolabilidad de la correspondencia es garantizar la libertad de las comunicaciones, es decir, impedir la injerencia de un tercero en el proceso de comunicación de dos o más personas, ya sea desde su acto inicial (impedir la comunicación) como en su desarrollo (interceptación). Este derecho incluye en su núcleo esencial la protección al secreto no solo del contenido de la comunicación, sino de los interlocutores, el lugar y el momento de realización. “El precepto parte de una presunción iuris et de iure de

que lo comunicado es secreto en un sentido sustancial (STC 117/1994, FJ 7.°)".[42] En este sentido, la inviolabilidad de correspondencia es un derecho autónomo pero instrumental pues garantiza también el derecho a la intimidad y a la privacidad de las personas.

En la Constitución de 1835 se establece por primera vez como una garantía del ciudadano la inviolabilidad de la correspondencia con límites establecidos en la ley: "Artículo 106.- La correspondencia epistolar es inviolable: no podrán abrirse ni interceptarse, ni registrarse los papeles o efectos, sino en los casos especialmente señalados por la ley". De este texto se destaca que la Constitución solo protegía la correspondencia epistolar, pero incluía papeles o efectos que no necesariamente eran parte del proceso de comunicación.

Más adelante, la Constitución Política de 1843 nuevamente consagra el derecho a la inviolabilidad de la correspondencia. Destaca la sanción a los empleados de correos, que no constaba en la Constitución anterior. La norma textualmente señala: "Artículo 100.- Es inviolable el secreto de las cartas; los empleados de la renta de correos serán responsables de la violación de esta garantía; fuera de los casos que prescriban las leyes". La palabra *secreto* se incluye en el texto constitucional como una de las garantías que protege este derecho. Esta norma restringe su alcance únicamente a la confidencialidad de las cartas, por lo tanto excluye los papeles y efectos de la persona, como constaba en el texto anterior.

Asimismo, el artículo señalado menciona elementos fundamentales del respeto a la inviolabilidad de correspondencia al señalar la prohibición de apoderamiento de documentos o papeles conforme consta descrito en la siguiente norma que se transcribe: "Artículo 101.- Está prohibido el apoderamiento injusto de los papeles, y correspondencias de cualquier ecuatoriano. La ley determinará en qué casos, y con qué justificación, pueda procederse a ocuparlos".

Para 1845, cuando la Convención dictaba en Cuenca la nueva Constitución, consta una norma respecto a la inviolabilidad de la correspondencia, que retoma el texto de la Constitución de 1835 incluyéndose los papeles y efectos; además se elimina la mención a los funcionarios de los correos que constaba en la Constitución de 1843: "Artículo 130.- La Correspondencia epistolar es inviolable; no podrán abrirse, ni interceptarse, ni registrarse los papeles o efectos de propiedad particular sino en los casos especialmente señalados por la ley".

En la Constitución Política de 1851 se unifica el derecho a la inviolabilidad del domicilio y la inviolabilidad de la correspondencia. La norma textualmente dice: "Artículo 112.- No podrá ser allanada la casa de ningún ecuatoriano, ni su correspondencia o papeles interceptados o registrados sino por la autoridad, en los casos y con las formalidades prescritas por la ley". Se omite la palabra *competente* respecto de la autoridad que emite la autorización legal que faculta la interceptación o registro de la correspondencia o papeles. Omisión que complica al texto constitucional pues las limitaciones al derecho, además de necesitar de reserva legal, deben provenir de autoridad jurisdiccional.

En el artículo 129 de la Constitución de 1852, y en el artículo 122 de la Constitución del año 1861, nuevamente se separan las normas sobre inviolabilidad de domicilio y de correspondencia conforme el contenido de la Constitución de 1845.

[42] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 306.

Asimismo, la estructura básica del artículo se repite en la Constitución de 1861; sin embargo, consta una alusión expresa a la invalidez procesal de usar como prueba las cartas en las causas sobre delitos políticos. La norma textualmente dice: "Artículo 122. La correspondencia epistolar es inviolable, y no hará fe en las causas sobre delitos políticos. No podrán abrirse, ni interceptarse, ni registrarse los papeles o efectos de propiedad particular, sino en los casos señalados por la ley". De esta precisión, puede concluirse que efectivamente este derecho tenía como finalidad proteger a la persona de persecuciones o injerencias sobre todo de carácter político. Esta Constitución consagra el artículo 123 que determina: "Queda abolida la pena de muerte para los delitos puramente políticos; una ley especial determinará estos delitos."; es decir, se intensifica la garantía de la inviolabilidad de correspondencia porque se preceptúa una ley que determinará cuáles son los delitos políticos. No obstante, las Constituciones de 1884, 1897, 1906, 1929 y 1954 no determinan estos delitos ni mencionan una norma que lo haga.[43]

En la Constitución conocida como Carta Negra de Junio de 1869 se elimina la mención a la validez procesal de las cartas en juicios por delitos políticos, y el texto es idéntico a las anteriores Constituciones ya citadas. La norma determina: "Artículo 107.- La correspondencia epistolar es inviolable. No podrán abrirse, ni interpretarse, ni registrarse los papeles o efectos de propiedad particular, sino en los casos señalados por la ley".

La Asamblea Nacional expide en 1878 una nueva Constitución Política que reconoce el derecho a la inviolabilidad y secreto de la correspondencia y demás papeles con lo que la norma vuelve a incluir en el contenido del derecho al secreto y los documentos personales. Asimismo, se establecen claramente las distintas acciones que pudieran vulnerar este derecho, de tal forma que las proscribe directamente en todas las fases del proceso de comunicación. El mencionado artículo señala: "Artículo 17.- La Nación garantiza a los ecuatorianos: [...] 3. La inviolabilidad y secreto de la correspondencia y demás papeles, los que no pueden abrirse, interceptarse, ni registrarse sino en los casos señalados por la ley...".

En el artículo 31 de la Constitución Política de 1884, expedida en Quito por la Asamblea Nacional, y en el artículo 19 de la Constitución Política de 1897, expedida en Quito por la Asamblea Nacional, nuevamente se elimina al *secreto* y se agregan los efectos en la invalidez probatoria de la correspondencia en las causas sobre infracciones políticas. Además, aparece por primera vez la referencia a la propiedad privada de los papeles o efectos que conforman la correspondencia epistolar, como si se buscara dejar de lado aquellos que estando en manos privadas son de carácter público.

El mencionado texto de la Constitución de 1897 dice: "Artículo 31.- La correspondencia epistolar es inviolable, y no hará fe en las causas por infracciones políticas. Prohíbase interceptar, abrir o registrar papeles o efectos de propiedad privada, excepto en los casos que la ley señale".

En la segunda etapa histórica, en el proyecto nacional mestizo, la Constitución Política de 1906 señala un texto similar a los constantes en las versiones anteriores, aunque sí realiza una variante significativa, pues pasa a ser una de las garantías individuales que el Estado garantiza a los ecuatorianos; es decir, se la considera derecho: "De las garantías individuales y políticas. Artículo 26.- El Estado garantiza a los ecuatorianos: [...] 9. La inviolabilidad de la correspondencia epistolar y telegráfica, la cual no hará fe en las causas políticas. En

[43] R. BORJA Y BORJA, *Derecho constitucional ecuatoriano*, 196.

consecuencia, prohíbase interceptar, abrir o registrar papeles o efectos de propiedad privada, excepto en los casos señalados por la ley...". Además, se incluye en el sistema de protección la correspondencia telegráfica, con lo que se allana el camino para que la protección no se refiera exclusivamente a la correspondencia, sino a la comunicación que puede realizarse por varios medios o tecnologías.

En la Constitución Política de 1929, en el Título XIII de las Garantías Fundamentales consta: "Artículo 151.- La Constitución garantiza a los habitantes del Ecuador, principalmente, los siguientes derechos: [...] 11. El secreto e inviolabilidad de la correspondencia epistolar, telegráfica y telefónica, la cual no hará fe en las causas por infracciones políticas. Prohíbase interceptar, abrir o registrar papeles, cartas, libros de comercio o efectos de propiedad privada, fuera de los casos expresamente señalados por la Ley. Se guardará siempre reserva acerca de los asuntos ajenos al objeto de la ocupación o examen...". Esta norma recoge varias novedades constitucionales.

En primer lugar, se incluye la comunicación telefónica en el ámbito de protección del derecho. Además entre los documentos a ser protegidos no solamente constan las tradicionales cartas o correspondencia, papeles o efectos sino que se añaden los *libros de comercio* como elemento que garantiza el resguardo de información comercial de las personas naturales y jurídicas. Finalmente, aparece la obligación de reserva en asuntos ajenos al motivo de la interceptación de correspondencia, con lo que la norma constitucional preserva la intimidad y privacidad de las personas y una posible transgresión del derecho al honor. Esto último resulta interesante a la luz de esta investigación, ya que manifiestamente expresa un afán de protección de la información personal, sensible e íntima de las personas.

En la Constitución Política de 1945, en un texto casi idéntico al anterior, se elimina la lista ejemplificativa de correspondencia por el genérico *en todas sus formas* lo que viabiliza cualquier tecnología que permita la comunicación entre personas dentro del alcance de protección de esta norma. El texto dice: "Artículo 141.- El Estado garantiza: [...] 9. El secreto e inviolabilidad de la correspondencia en todas sus formas, la que no hará fe en las causas por delitos políticos. Prohíbese interceptar, abrir o registrar papeles, libros de comercio, cartas y demás documentos privados, fuera de los casos y en la forma que fije la ley. Se guardará reserva acerca de los asuntos ajenos al objeto del registro o examen".

En la Constitución Política de 1946, en el título denominado "Garantías individuales comunes", aparece el siguiente texto muy similar al anterior en contenido, ya que se protege la "correspondencia postal o de cualquier otra clase". También, elimina nuevamente la palabra "secreta" y la reserva de los asuntos ajenos y la invalidez probatoria para delitos políticos que expresamente se mencionaba en versiones anteriores: "Artículo 187.- El Estado garantiza a los habitantes del Ecuador: [...] 7. La inviolabilidad de la correspondencia postal o de cualquiera otra clase. En consecuencia, prohíbese interceptar, abrir o registrar la correspondencia ajena, excepto en los casos señalados por la ley...".

En la Constitución Política de 1967, en el Capítulo II, "De los derechos de la persona", se incluye el siguiente texto: "Artículo 28.- Derechos garantizados.- Sin perjuicio de otros derechos que se deriven de la naturaleza de la persona, el Estado le garantiza: [...] 10. La inviolabilidad de la correspondencia y el secreto de las comunicaciones teleféricos y telefónicas. Prohíbese abrir o registrar papeles, libros de comercio, cartas y más documentos privados, fuera de los casos y en la forma que la ley determine. Se guardará reserva sobre los asuntos ajenos al objeto del registro o examen. Los documentos obtenidos con violación de

esta garantía no harán fe en juicio". Al respecto, la norma señala que el derecho consiste en *la inviolabilidad de la correspondencia y el secreto de las comunicaciones*; es decir, se transgrede la correspondencia con su apertura, pero acerca de las comunicaciones pareciera que por la redacción de la norma solo existe violación cuanto se afecta su secreto mediante la interceptación. Esta sutil diferenciación, lejos de favorecer el contenido del derecho, puede permitir formas de transgresión que contrarían el espíritu de la norma, ya que tanto la inviolabilidad como el secreto son parte de la protección de las comunicaciones en el que la epistolar es una más. Asimismo, se dejan nuevamente de lado los términos genéricos y vuelven a ejemplificarse los documentos objeto de protección de este derecho: libros de comercio, cartas y más documentos privados; se añade una referencia a la ley para determinar su ejercicio. Con el afán de incluir todas las tecnologías se realiza la precisión de que las comunicaciones son teleféricos y telefónicas. La tecnología teleférico hace referencia a aquellas que dependían de cables colgantes.

El texto incluye una referencia al valor probatorio nulo, como garantía de un debido proceso, de aquellos documentos obtenidos con violación de la correspondencia. Esta referencia supera la omisión que hiciera la Constitución anterior; además señala que esta garantía es aplicable a toda clase de juicios y no únicamente a los relativos a delitos políticos como históricamente se había abordado el tema.

La Comisión de la Constitución debatió sobre ese particular. Por su parte, el honorable Arízaga Vega expresó que "en el proyecto del Partido Conservador hay un concepto que es muy útil, dada la forma como actúa la política en nuestro país. Muchas veces, dice, se viola la correspondencia y por esa causa se presentan acusaciones terribles contra las personas. Juzga conveniente incluir a continuación de este último numeral aprobado un inciso que diría: «las pruebas obtenidas con violación de esta garantía no harán fe en caso de delitos políticos»".[44] Mientras que el honorable Corral Borrero sugirió que no solo se limite la invalidez probatoria de estos documentos a los juicios políticos, sino en juicios penales, civiles, laborales, entre otros, en garantía de la legalidad y validez de la prueba.[45] Como consta del texto de la norma finalmente aprobada, se aprobó una redacción abierta que manifiestamente pretende que cualquier documento obtenido mediante la violación de la correspondencia no hará fe en juicio cualquiera que sea la naturaleza de la acción planteada.

Adicionalmente, en los debates de la Comisión de la Constitución, al referirse a las excepciones que facultan abrir o registrar papeles, libros de comercio, cartas y más documentos privados, se discutió "que en vez de las palabras «fuera de los casos y en la forma que determine la ley», que es un concepto general, se diga «fuera de los casos en que se dicte auto judicial en contrario», a fin de evitar los abusos que han ejercido las autoridades administrativas por motivos políticos".[46] Julio César Trujillo, por su parte, sostuvo mantener el artículo sin la alusión al auto judicial debido a que "la inviolabilidad absoluta de la correspondencia no puede existir, dado que en una carta se puede introducir un contrabando, y mucho más en paquetes postales";[47] es decir, explicitó la necesidad de mantener en la redacción *la reserva legal*, por la cual se puedan establecer excepciones a la inviolabilidad de correspondencia. Ya que, mediante estas particularidades expresamente establecidas en la ley, el Estado puede cumplir con su deber de garantizar tanto la seguridad ciudadana como el seguimiento de los deberes fiscales de los particulares, entre otros. Para ello, utilizó al

[44] COMISIÓN DE LA CONSTITUCIÓN DE ECUADOR DE 1967, [Acta No. 155], 2.
[45] ASAMBLEA NACIONAL CONSTITUYENTE DE 1967 DE ECUADOR, [Acta No. 47], 34.
[46] COMISIÓN DE LA CONSTITUCIÓN DE ECUADOR DE 1967, [Acta No. 155], 2.
[47] Ibíd.

contrabando como ejemplo, ya que tiene tanto repercusiones penales como administrativas. Esta argumentación permitió que la norma conserve la alusión a la reserva de ley en términos generales.

Acerca de la Constitución de 1978, en su versión original señalaba: "Título II De Los Derechos, Deberes y Garantías. Sección I. De los derechos de la Persona. Artículo 19.- Toda persona goza de las siguientes garantías: [...] 7. La inviolabilidad y el secreto de la correspondencia. Sólo puede ser ocupada, abierta y examinada en los casos previstos por la ley. Se guarda secreto de los asuntos ajenos al hecho que motivare su examen. El mismo principio se observa con respecto a las comunicaciones telegráficas, cablegráficas y telefónicas. Los documentos obtenidos con violación de esta garantía no hacen fe en juicio...". Se dejan de lado precisiones innecesarias y nuevamente la norma tiene por objeto proteger la inviolabilidad y el secreto de la correspondencia; líneas abajo aclara que las comunicaciones que también se cobijan bajo este precepto son las telegráficas, cablegráficas y telefónicas. Se añade una nueva tecnología de comunicación: la cablegráfica. Se omite la descripción de los documentos materia de protección y se mantiene una redacción generalizada.

En la Primera Codificación de la Constitución Política de1978 consta un texto casi idéntico al anterior, pero en lugar de autorizar que la correspondencia sea *ocupada*, la norma faculta que esta sea *aprehendida*; en otros términos, deja de utilizarse un vocablo común que puede causar equívoco (ocupada) y opta por usar un término técnico procesal pertinente por el cual se garantiza prueba debidamente obtenida dentro de un proceso judicial (aprehendida). El texto dice: "Artículo 19.- Sin perjuicio de otros derechos necesarios para el pleno desenvolvimiento moral y material que se deriva de la naturaleza de la persona, el Estado le garantiza: [...] 8. La inviolabilidad y el secreto de la correspondencia. Sólo podrá ser aprehendida, abierta y examinada en los casos previstos por la ley. Se guardará secreto de los asuntos ajenos al hecho que motivare su examen. El mismo principio se observará con respecto a las comunicaciones telegráficas, cablegráficas y telefónicas. Los documentos obtenidos con violación de esta garantía, no harán fe en juicio...". Como se analizó anteriormente, otra variante es la parte general del artículo 19 que se refiere a derechos de las personas y ya no a garantías.

La Segunda Codificación de la Constitución Política de 1978 señala un texto exactamente igual a la codificación anterior.

En la Tercera Codificación de la Constitución Política de 1978, en el Título II, "De los derechos, deberes y garantías", Sección I, "De los derechos de las personas", Principios generales, consta lo siguiente: "Artículo 22.- Sin perjuicio de otros derechos necesarios para el pleno desenvolvimiento moral y material que se deriva de la naturaleza de la persona, el Estado le garantiza: [...] 9. La inviolabilidad y el secreto de la correspondencia. Solo podrá ser aprehendida, abierta y examinada en los casos previstos en la Ley. Se guardará secretos de los asuntos ajenos al hecho que motivare su examen. El mismo principio se observará con respecto a las comunicaciones telegráficas, cablegráficas, telefónicas, electrónicas y otras similares. Los documentos obtenidos con violación de esta garantía no harán fe en juicio y los responsables serán sancionados conforme a la Ley...". El texto es casi idéntico a la versión original, a la primera y segunda codificación, excepto porque dentro de las comunicaciones protegidas al amparo de esta norma constitucional consta la *electrónica*, además se utiliza una frase genérica que engloba a las otras tecnologías que se desarrollen. Adicionalmente, se

menciona la invalidez probatoria de los documentos obtenidos irrespetando la garantía de inviolabilidad y secreto.

Se añade la constancia de que la responsabilidad por la transgresión de este derecho se determinará en la ley. En el Código Penal de la época se señala que "el secreto de la correspondencia puede ser afectada por la actuación ilegal de las autoridades o de personas particulares; ambas infracciones están sancionadas por el Código Penal (artículo 197 a 202)".[48]

La transcripción del texto antes analizado aparece en la Cuarta Codificación de la Constitución Política de 1978.

Sobre la Constitución Política de 1998, Título III, "De los derechos, garantías y deberes", Capítulo 2, "De los derechos civiles", en el siguiente texto se señala: "Artículo 23.- Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: [...] 13. La inviolabilidad y el secreto de la correspondencia. Esta sólo podrá ser retenida, abierta y examinada en los casos previstos en la ley. Se guardará el secreto de los asuntos ajenos al hecho que motive su examen. El mismo principio se observará con respecto a cualquier otro tipo o forma de comunicación". Nuevamente la parte general del artículo se modifica a favor de reconocer y garantizar no solo los derechos que constan en la propia Constitución, sino en los instrumentos internacionales vigentes. Se omite el término *aprehendida* y se utiliza *retenida*. Se abre la norma para que este principio proteja cualquier forma de comunicación. Se omite mencionar el valor probatorio de los documentos obtenidos y los niveles de responsabilidad establecidos en la ley.

Finalmente, en la Constitución de la República del Ecuador de 2008, en el Título II, "Derechos", Capítulo segundo, "Derechos del buen vivir", Capítulo sexto, "Derechos de libertad", consta el siguiente texto: "Artículo 66.- Se reconoce y garantizará a las personas: [...] 21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen". Este derecho protege cualquier otro tipo o forma de comunicación, pues se menciona la correspondencia virtual, así como la constancia de la necesidad de intervención judicial previa que deberá valorar si los hechos del caso están previstos en la ley.

En esta Constitución aparece la mención expresa de los derechos que se limitan en un estado de excepción conforme el "Artículo 165.- Durante el estado de excepción la Presidenta o Presidente de la República únicamente podrá suspender o limitar el ejercicio del derecho a la inviolabilidad de domicilio, inviolabilidad de correspondencia, libertad de tránsito, libertad de asociación y reunión, y libertad de información, en los términos que señala la Constitución". La Constitución de 2008 al enumerar los derechos que pueden ser suspendidos en un estado de excepción menciona expresamente a la inviolabilidad de la correspondencia, ya que con el estado actual de avance en las tecnologías de la información y comunicación uno de los mecanismos indispensables para afrontar una agresión, un conflicto armado, internacional o interno, conmoción interna, calamidad pública o un desastre natural es la posibilidad de monitorear las comunicaciones de los ciudadanos; en sentido contrario, si las causas de estado de excepción no existen, el Estado no puede bajo ningún concepto —ni aun

[48] J. TOBAR DONOSO Y J. LARREA HOLGUÍN, *Derecho constitucional ecuatoriano*, 234.

por garantizar la seguridad ciudadana— realizar este monitoreo pues afectaría directamente las libertades ciudadanas y la democracia.

En la Mesa No. 1 de la Constituyente se realizó la siguiente exposición que describe el espíritu con el que se adoptó en el vigente texto constitucional este derecho:

> El derecho al secreto e inviolabilidad de las comunicaciones, forma parte integrante de los llamados derechos de la personalidad y, por tanto, íntimamente relacionados con el derecho a la intimidad, al honor, a la reputación, entre otros. Podemos observar que el derecho al secreto y a la inviolabilidad de las comunicaciones y documentos privados, constituye un derecho fundamental estrechamente vinculado al derecho a la intimidad, pues, este es, el bien jurídico tutelado, cuya finalidad es proteger a la persona de cualquier intromisión proveniente de particulares, así como de funcionarios o autoridades en sus comunicaciones y documentos privados, derechos estos, recogidos no exclusivamente, por nuestra ley fundamental, sino también en instrumentos internacionales sobre derechos humanos. Sin embargo, si bien son derechos humanos, no son de carácter absoluto, por cuanto la propia Constitución y la ley, sobre la sobreprotección a la privacidad de las comunicaciones, admite excepciones, así, siempre que medie autorización judicial, pueden abrirse, interceptarse o intervenirse las comunicaciones con las garantías previstas en la ley.[49]

De esta cita es importante destacar la relación que los propios asambleístas constituyentes edificaron respecto del derecho a la inviolabilidad de la correspondencia y el derecho a la intimidad, el honor, la reputación, de tal forma que se evidencia la instrumentalidad y relación integral del primero respecto de los otros derechos, por lo que su transgresión significa la vulneración directa de todo el sistema de protección de la privacidad y del libre desarrollo de la personalidad.

Además, en este segundo debate constitucional se reiteró la relación de la inviolabilidad de la correspondencia con la intimidad, pero además se mencionó que este derecho no garantiza únicamente las transgresiones producidas por particulares, sino también por funcionarios o autoridades, lo que da cuenta de que conforme a la historia ecuatoriana nuevamente este derecho se consagra como garantía del ejercicio democrático de libertad de conciencia, de expresión y de opinión política. El texto en mención expresamente señala: "La inviolabilidad de correspondencia, que es un principio universal, derecho estrechamente vinculado a la intimidad, pues éste es el bien jurídico tutelado, cuya finalidad es proteger a la persona de cualquier intromisión proveniente de particulares, así como de funcionarios o autoridades en sus comunicaciones y documentos privados".[50]

En el segundo debate se añade en el texto constitucional "la intervención judicial antes de cualquier medida, legalmente reconocida que vaya en contra de este derecho".[51] Sin duda, la única autoridad competente para resolver una autorización de interceptación es un juez que además deberá motivar suficientemente su decisión debido a que esta acción transgrede un sinnúmero de derechos como vimos líneas arriba.

Luego del relato cronológico de la forma en que las distintas Constituciones han recogido el derecho de la inviolabilidad de la correspondencia, podemos concluir que aparece en la Constitución de 1835, es decir una después que aquella que recoge la inviolabilidad del domicilio (Constitución de 1830). A partir de entonces, su importancia es tal que no se omite

[49] ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 50], 59.
[50] Ibíd., [Acta No. 64], 42.
[51] Ibíd., 21.

en adelante. Es más, su contenido va ampliándose a medida que avanza el período republicano, ya que siendo años convulsos por la represión y reforzamiento del predominio latifundista clerical[52] se volvía indispensable su vigencia en protección de la libertad ideológica y política, de tal forma que incluso existe alusión expresa a la invalidez procesal de usar como prueba las cartas obtenidas sin autorización judicial en las causas sobre delitos políticos.

La forma de conceptualizar el derecho evoluciona, ya que no solo protege la apertura, el registro sino la interceptación y la apropiación, ya no solo de correspondencia epistolar sino de los papeles o efectos de propiedad particular, aunque estos no sean parte de un proceso de comunicación. Sin duda, esta forma de pensar a la inviolabilidad de correspondencia manifiesta abiertamente que una de sus finalidades es la protección del secreto, y por ende de aquella zona de privacidad e intimidad a la que todo ser humano tiene derecho, aunque en ese momento histórico no se haya concebido como tal.

Otro de los temas de continua movilidad en los textos constitucionales de los primeros años de la república era la referencia a la *autoridad competente* para permitir el acceso autorizado o la interceptación o registro de la correspondencia o papeles. En los primeros textos se permitía tal facultad a *funcionarios competentes* cuando en garantía del debido proceso la autorización provenía exclusivamente del *juez competente*.

En la segunda etapa histórica, el proyecto nacional mestizo, la Constitución Política de 1906 incluye a la inviolabilidad de correspondencia entre las garantías individuales que el Estado reconoce a los ciudadanos. Además, a partir de esta Constitución, la protección constitucional varía desde realizar un enlistamiento de las distintas tecnologías de comunicación, incluyendo la telegráfica, telefónica, teleférica, o utilizar frases genéricas que incluyan todas las formas de tecnología existentes y que pudieran llegar a existir. Sin duda, esta forma genérica de redacción es más proteccionista pues evita dejar por fuera algún tipo de tecnología.

Asimismo, no solo es parte del sistema de protección las cartas o correspondencia, papeles o efectos sino que se incorporan los libros de comercio; pero además se establece la prohibición expresa de divulgar aquella información sobre asuntos ajenos al motivo de la interceptación de correspondencia. De tal manera que a través de esta prohibición se intenta cerrar el círculo de protección, pues este derecho resguarda también el secreto, y por ende y aunque sin decirlo, protege la privacidad y la intimidad e incluso una posible transgresión del derecho al honor.

En la tercera etapa histórica del proyecto nacional de la diversidad se incluyen otras tecnológicas como la *cablegráfica y la electrónica*, hasta finalizar con una redacción general que señala comunicación *física y virtual* con la que se intenta expresar en la materialidad o no de las comunicaciones, todos los tipos de tecnologías amparadas por el derecho.

Más importante es la ampliación de la invalidez probatoria de los documentos e información obtenida de un registro, o interceptación ilegal, no solo para juicios políticos sino para todo tipo de juicios. Y además, no es suficiente la sola autorización de la ley para permitir el registro o la interceptación de las comunicaciones, sino que es indispensable la intervención judicial que valore si los hechos del caso están previstos en la ley.

[52] E. AYALA MORA, *Historia, tiempo y conocimiento*, 117.

Todo lo dicho da cuenta de la conexión e importancia directa de la inviolabilidad de la correspondencia respecto del derecho al secreto, a la privacidad, a la intimidad y al honor, más aún cuando el acceso a ciertos documentos o información pueden afectar directamente el ejercicio de otras libertades individuales como la ideológica, religiosa, política, su libre desarrollo de la personalidad o influir directamente en el debido proceso, y por ende en la imputación errónea o falsa de un delito.

2.4 Derecho al honor (1845)

Si bien la honra responde en un primer momento a una estratificación de clases, ya que solo los nobles o aquellas personas que pertenecían a las élites de gobierno tenían un honor que proteger, la Constitución democrática se apropió de esta categoría mediante la dignidad humana y le otorgó un sentido igualitario. "Se trata de asegurar a toda persona que pueda acceder al reconocimiento social, a la estima de los demás entendida como capacidad de aparecer ante ellos, y participar con ellos, en condiciones de semejanza como garantía de la posibilidad de participación en el espacio social. De este modo, sólo cuando tales posibilidades quedaran afectadas o condicionadas, se produciría una vulneración del derecho".[53] Entonces, el honor está directamente relacionado con los valores sociales y las costumbres vigentes en cada época.[54]

Las primeras formas de protección al honor se encuentran en el Derecho Romano con la *actio iniuriarum* (acción contra las injurias). Posteriormente, aparecen en las VII Partidas de Alfonso X las deshonras punibles y las no punibles. En los textos contemporáneos aparece en el artículo 12 de la Declaración Universal de los Derechos Humanos cuando se señala que: "Nadie será objeto de [...] ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias y ataques". En el Convenio Europeo de los Derechos Humanos no aparece, en cambio, un artículo que recoja de manera autónoma el derecho al honor, sino que solo se menciona que "podrá ser sometida a ciertas restricciones que constituyan medidas necesarias en una sociedad democrática para la protección, entre otros aspectos de la reputación o derecho ajenos".[55]

Actualmente, el honor se lo considera junto a la intimidad personal y familiar, a la propia imagen y voz, como elementos constitutivos de la dignidad de la persona e instrumentos indispensables para el libre desarrollo de la personalidad. De tal forma que no pueden ser transgredidos ni siquiera por voluntad propia.[56] Dicho esto, el honor desde la perspectiva de la privacidad y la intimidad está directamente relacionado con esta investigación sobre los antecedentes del derecho a la protección de datos personales. Tanto más que, como veremos posteriormente, en Ecuador la jurisprudencia constitucional referencial, aquella dictada antes de la vigente Constitución de 2008, establecía que el *habeas data* se convierte en garantía jurisdiccional de estos derechos de la personalidad.[57]

A continuación se realizará una revisión histórico-constitucional respecto del derecho al honor en Ecuador. Es a finales del primer período histórico, del proyecto nacional criollo, en

[53] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 699.
[54] M. ENCABO VERA, *Derechos de la personalidad* (Madrid: Marcial Pons, 2012), 89.
[55] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 696.
[56] M. CARRASCO DURÁN Y J. PÉREZ ROYO, *Curso de derecho constitucional* (Barcelona: Atelier, 2012), 291-2.
[57] Ecuador. TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0007-2006-HD]; [Sentencia No. 0070-2003-HD].

el año 1845, cuando por primera vez se reconoce el derecho al honor en la Constitución. La norma que recoge este derecho se transcribe: "Artículo 116.- Todo ciudadano se presume inocente y tiene derecho a conservar su buena reputación, mientras no se le declare delincuente conforme a las leyes". En líneas generales, consta esta forma de reconocimiento, con pequeñas variaciones que veremos a continuación, en las Constituciones de 1851, 1929, 1945 y 1946; estas tres últimas Constituciones pertenecientes al segundo período republicado, del proyecto nacional mestizo.

Por la secuencia histórica cabe decir que la Constitución de 1884 menciona a la honra únicamente desde la libertad de expresión. El texto dice: "Artículo 28.- Todos pueden expresar libremente sus pensamientos de palabra o por la prensa, respetando la Religión, la decencia, la moral y la honra, y sujetándose, en estos casos, a la responsabilidad legal". Es decir, esta Constitución omite el derecho a la honra, ni aún atada al principio de inocencia, menos aún como derecho autónomo protegido por el Estado, sino que la establece como limitación al derecho a la libertad de expresión.

La variante más importante durante estos años fue el texto de la Constitución Política de 1929, que ubica al derecho al honor en el título relativo a las garantías fundamentales de los habitantes del Ecuador: "Artículo 151: "La Constitución garantiza a los habitantes del Ecuador, principalmente, los siguientes derechos: [...] 3. El derecho de ser presumido inocente y de conservar honor y buena reputación, mientras no haya declaración de culpabilidad, conforme a las leyes".

Esos preceptos constitucionales sostienen que el derecho a una buena reputación se garantiza solo desde la perspectiva del principio de inocencia; es decir, la persona era honorable únicamente cuando no había cometido un delito sancionado con sentencia penal ejecutoriada. En este contexto, el derecho a la honra no se concebía como uno de los derechos de la personalidad entendidos como "instrumentos para la conservación de la autonomía de cada persona en sus relaciones sociales",[58] sino que estaba directamente relacionado con el principio de inocencia y a la necesidad de una sentencia que le impute responsabilidad penal que le prive de honor.

En la Constitución Política de 1945, en el Título Décimo Tercero, "De las garantías fundamentales", Sección Primera, "De los derechos individuales" se señala: "Artículo 141.- El Estado garantiza: [...] 3. El ser presumido inocente y conservar la honra y la buena reputación, mientras no haya declaración judicial de responsabilidad conforme a las leyes. Nadie puede ser obligado a prestar testimonio en juicio penal contra su cónyuge o sus parientes dentro del cuarto grado de consanguinidad o segundo de afinidad, ni compelido, con juramento o por medio de apremio, a declarar contra sí mismo en asuntos que comporten responsabilidad penal. Prohíbanse las penas infamantes...". Esta norma, además de la vinculación con el principio de inocencia, incluye la prohibición de testimoniar en contra de sí mismo o de miembros de su familia, lo que no es parte del derecho al honor sino del debido proceso.

Adicionalmente, dicha Constitución establece en el artículo 141, numeral 10, lo siguiente: "El Estado garantiza: [...] 10. La libertad de opinión, cualesquiera que fueren los medios de expresarla o difundirla. La injuria, la calumnia y toda manifestación inmoral, están sujetas a

[58] M. CARRASCO DURÁN Y J. PÉREZ ROYO, *Curso de derecho constitucional*, 286.

las responsabilidades de ley". En esta norma, la transgresión de la libertad de opinión se materializa en las injurias cuando en realidad estas son formas típicas de atropello a la honra.

En la normativa constitucional de 1946 no consta el derecho a la honra en la lista de garantías individuales comunes de responsabilidad del Estado. Aparece exclusivamente la libertad de expresión: En la Sección II, Garantías individuales comunes, en el artículo 187, numeral 11, se dice:

> Artículo 187.- El Estado garantiza a los habitantes del Ecuador: [...] 11. La libertad de expresar el pensamiento, de palabra, por la prensa o por otros medios de manifestarlo y difundirlo, en cuanto estas manifestaciones no impliquen injuria, calumnia, insulto personal, sentido de inmoralidad o contrario a los intereses nacionales, actos que estarán sujetos a las responsabilidades y los trámites que establezca la ley. La Ley regulará el ejercicio de esta libertad, tomando en cuenta que el periodismo tiene por objeto primordial la defensa de los intereses nacionales y constituye un servicio social, acreedor al respeto y apoyo del Estado.

Nuevamente la honra, mediante la injuria, la calumnia o el insulto personal aparece como limitación a la libertad de expresión y no como transgresión inmediata del derecho al honor.

En otro artículo de este mismo cuerpo normativo consta la obligación del Estado de rehabilitar a los condenados injustamente para recuperar la honra mancillada por la indebida atribución de un delito. La norma textualmente dice: "Artículo 45.- Son atribuciones exclusivas de la Cámara del Senado: [...] 4. Rehabilitar, establecida la inocencia honra o la memoria de los condenados injustamente...".

En el tercer período republicano, el del proyecto nacional de la diversidad por intermedio de la Constitución de 1967, reconoce por primera vez el derecho a la honra sin vincularla o materializarla con el principio de inocencia o asociarla a un indebido ejercicio de la libertad de opinión. Su tenor literal aparece en el Capítulo II, Título "De los derechos de la persona": "Artículo 28.- Derechos garantizados. - Sin perjuicio de otros derechos que se deriven de la naturaleza de la persona, el Estado le garantiza: [...] 4. El derecho a la honra y a la intimidad personal y familiar".

Pese a lo dicho, en la misma Constitución el artículo 28, numeral 5, nuevamente se menciona a la libertad de opinión y la de expresión como derecho de la persona, estableciendo como uno de los límites a la honra de las personas; es decir, sigue considerándose a la honra como limitación que impide un ejercicio indebido de este derecho.

Respecto de la honra, esta Constitución la concibe como un derecho autónomo, aunque aparece acompañada del derecho a la intimidad, que también se reconoce en esta Constitución por primera vez. Estos dos derechos pudieron consagrarse en numerales independientes y no en mismo numeral, de tal forma que tal como consta en el texto se vislumbran como complementarios, en el afán de proteger el libre desarrollo de la personalidad.

La Comisión de la Constitución que presentó la propuesta original, que posteriormente fue aprobada por los asambleístas constituyentes, discutió sobre varios aspectos que pasamos a analizar a continuación, pues ayudan a identificar el espíritu de la disposición.

Originalmente, la Comisión reconocía al honor como el derecho garantizado. Sin embargo, cambió de opinión luego de la intervención del honorable Villacrés, quien sostuvo que el

derecho que debe salvaguardarse es la honra por cuanto: "tiene una observación, y es que lo que protege la ley no es el honor de la persona sino la honra. Dice que los autores hacen distinción de estos dos términos, y que la honra hace relación con la buena fama, la buena reputación; en cambio que el honor es ya otro concepto, pues una persona sin honra tiene honor".[59]

Resulta clásica la división en honor y honra. Honor es el "concepto particular y propio que cada persona tiene de sí", significa "estima y respeto de la dignidad propia...".[60] Acerca de la honra o buena reputación o dignidad personal, esta se refiere a la estimación y reconocimiento social del valor que corresponde a una persona intachable.[61] Consiste en la "cualidad moral que lleva al más severo cumplimiento de los derechos ante los demás y nosotros mismos. Se traduce en gloria, buena reputación que sigue a la virtud...".[62] La Convención Americana de Derechos Humanos o Pacto de San José en el artículo 11 señala que "toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad".

Otros autores entre los cuales destacan Bernal del Castillo[63], Ochoa[64] y Bonilla[65] señalan que es el honor el derecho, y que es respecto de este, que existe una división entre subjetivo y objetivo que coincide como veremos en los contenidos de honra y honor señalados.

El honor objetivo, también llamado reputación, es el que haría las veces de honra según las conceptualizaciones antes citadas. Ya que es el relativo a "la valoración que otros hacen de la personalidad ético social de un sujeto"[66] y "consiste en la fama, buen nombre o reputación de que goza ante los demás una determina persona";[67] por lo tanto, carece de objetividad. Su contenido se construye desde las ideas, las normas, los valores, las costumbres y las preocupaciones vigentes en determinado lugar y época[68] en una sociedad; de tal manera que hay algo convencional y arbitrario en las cualidades morales que la idealizan.[69]

En cambio, el honor subjetivo se refiere al concepto propio de honor, ya que su contenido refiere a la autovaloración[70] o el aprecio de la propia dignidad; en consecuencia es una cualidad invariable inherente a la naturaleza y dignidad humana.[71] Cada individuo realiza una elaboración propia de los elementos que integran su honor y en tales condiciones se determina su subjetividad; cada persona tendrá sus propias tablas de valoración. Su transgresión se materializa en el insulto que puede recibir una persona en privado, de tal forma que habrá transgresión al honor subjetivo,[72] pero no al honor objetivo para el cual es necesario que el agravio se efectué frente a otros, quienes cambien su percepción respecto de su valoración en un entorno social.

---

[59] COMISIÓN DE LA CONSTITUCIÓN DE ECUADOR DE 1967, [Acta No. 154], 3.
[60] S. E. CIFUENTES, *Derechos personalísimos*, 3a. ed. actualizada y ampliada (Buenos Aires: Editorial Astrea de A. y R. DePalma, 2008), 489.
[61] A. VALENCIA ZEA, *Derecho civil*, vol. I (Bogotá: Temis, 1966), 388.
[62] S. E. CIFUENTES, *Derechos personalísimos*, 489.
[63] J. BERNAL DEL CASTILLO, *Honor, verdad e información*, (España: Universidad de Oviedo, 1994), 59-60
[64] G. OCHOA, *Derecho civil I: personas*, (Venezuela: Universidad Católica Andrés, 2006), 479-481.
[65] J. BONILLA, *Personas y derechos de la personalidad*, (España: Reus, 2010), 98-101.
[66] S. E. CIFUENTES, *Derechos personalísimos*, 488.
[67] E. ÁLVAREZ CONDE, *Curso de Derecho constitucional*, vol. I (Madrid: Tecnos, 2008), 432.
[68] M. OSSORIO Y FLORIT, *Enciclopedia Jurídica Omeba*, vol. XIV (Omeba), 470.
[69] S. E. CIFUENTES, *Derechos personalísimos*, 488.
[70] C. A. GHERSI, *Derecho civil: parte general*, 3a. ed. actualizada y ampliada (Buenos Aires: Editorial Astrea de Alfredo y Ricardo DePalma, 2002), 247.
[71] S. E. CIFUENTES, *Derechos personalísimos*, 488.
[72] C. A. GHERSI, *Derecho civil*, 247.

De Cupis unifica ambas vertientes y define al honor como "el íntimo valor del hombre, la estima de terceros o bien la consideración social, el buen nombre o buena fama, así como el sentimiento o consciencia de la propia dignidad".[73]

Finalmente, la doctrina, la normativa y la jurisprudencia establecen tres conceptos que conforman el derecho al honor: dignidad, fama y propia reputación;[74] así como, dos formas de intromisiones ilegítimas que verifican su transgresión. La primera, la imputación de hechos verdaderos o falsos, y por lo tanto, verificables; de tal forma, que solo existe transgresión del derecho a la honra cuando la imputación es falsa. La segunda, la manifestación de juicios de valor, que por no ser verificables no pueden ser ni verdaderos ni falsos; en consecuencia, no se verifica transgresión del derecho al honor sino que podría producirse una intromisión ilegítima en el derecho a la intimidad o a la propia imagen.[75]

La normativa legal en general ha determinado los delitos de injuria y de calumnia como mecanismos de protección de la honra de las personas. La *injuria* es toda expresión o acción que causa deshonra, descrédito o menosprecio; mientras que *calumnia* es la falsa imputación de un delito[76]. Esta última acción dolosa provoca una sanción penal[77]. Tanto la injuria como la calumnia pueden ser causa de indemnización civil que compense los daños materiales y morales sufridos por la víctima[78].

La norma aprobada por la Comisión Constitucional reconocía el derecho a la honra. No fue un término que causó discusión en los debates de aprobación del texto constitucional por parte de la Asamblea Constituyente. Únicamente, el honorable Villacrés Miranda informó a todos los presentes del cambio que se produjo respecto de la propuesta original de la Comisión y justificó la protección de la honra y no del honor por cuanto "lo que garantizaba la ley es el fuero moral, la integridad personal del individuo...",[79] argumentos que no fueron controvertidos y que permitieron la aprobación del texto. Entendemos que al mencionar el

[73] Citado por E. ÁLVAREZ CONDE, *Curso de Derecho constitucional*, vol. 1, 432.
[74] En este sentido Cifuentes manifiesta: "La personalidad está sostenida en la reputación; crece, se agranda con la fama y el esfuerzo para consolidarla ante los demás; depende de la opinión ajena, pero también de la estima personal". S. E. CIFUENTES, *Derechos personalísimos*. El derecho al honor implica la protección de la propia estimación del buen nombre y la reputación (STC 43/1981), incluida la reputación profesional (STC223/1992).
[75] M. CARRASCO DURÁN Y J. PÉREZ ROYO, *Curso de derecho constitucional*, 292.
[76] A. ALESSANDRI RODRÍGUEZ, M. SOMARRIVA UNDURRAGA, A. VODANOVIC H. Y A. ALESSANDRI RODRÍGUEZ, *Tratado de derecho civil: partes preliminar y general* [6. ed.], 1. ed., (Santiago: Editorial Jurídica de Chile), 489.
[77] ASAMBLEA NACIONAL DEL ECUADOR, [Código Orgánico Integral Penal, ROS, No. 180 (10 de febrero de 2014), Última modificación: 03 de junio de 2019]: "Artículo 182.- Calumnia.- La persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años. No constituyen calumnia los pronunciamientos vertidos ante autoridades, jueces y tribunales, cuando las imputaciones se hubieren hecho en razón de la defensa de la causa. No será responsable de calumnias quien probare la veracidad de las imputaciones. Sin embargo, en ningún caso se admitirá prueba sobre la imputación de un delito que hubiere sido objeto de una sentencia ratificatoria de la inocencia del procesado, de sobreseimiento o archivo. No habrá lugar a responsabilidad penal si el autor de calumnias, se retractare voluntariamente antes de proferirse sentencia ejecutoriada, siempre que la publicación de la retractación se haga a costa del responsable, se cumpla en el mismo medio y con las mismas características en que se difundió la imputación. La retractación no constituye una forma de aceptación de culpabilidad".
[78] ASAMBLEA NACIONAL DEL ECUADOR, [Código Civil Codificado, ROS, No. 46 (24 de junio de 2005), Última modificación: 8 de julio de 2019]: "Artículo 2231.- Las imputaciones injuriosas contra la honra o el crédito de una persona dan derecho para demandar indemnización pecuniaria, no sólo si se prueba daño emergente o lucro cesante, sino también perjuicio moral".
[79] ASAMBLEA NACIONAL CONSTITUYENTE DE 1967 DE ECUADOR, [Acta No. 47], 37.

fuero moral lo que realizó el asambleísta es coincidir con la visión de que la honra se refiere a la percepción que una sociedad, desde sus propias premisas morales, tiene respecto de un individuo.

Respecto de la Constitución de 1978, en su versión original señalaba: "Artículo 19.- Toda persona goza de las siguientes garantías: [...] 3. El derecho al honor y a la buena reputación. Toda persona que fuere afectada por afirmaciones inexactas o agraviada en su honor, por publicaciones hechas por la prensa u otros medios de comunicación social, tiene derecho a que éstos hagan la rectificación correspondiente en forma gratuita...". La nueva norma constitucional ahora consagra el honor en lugar de la honra y añade a la buena reputación.

Además, relaciona directamente la forma de transgresión del derecho al honor a través de los medios de comunicación y no al de libertad de expresión, de ahí la referencia expresa al derecho de rectificación. En la Constitución de 1945, el texto era muy similar al anteriormente transcrito "pero en referencia a imputaciones falsas o injuriosas; el texto de la nueva es ligeramente más amplio, ya que menciona aún lo simplemente «inexacto», no sólo lo falso".[80] Esta relación del derecho al honor y del derecho a la libertad de expresión, si bien plantean una visión interesante sobre los límites, causas y consecuencias, sin embargo, no permite una adecuada delimitación del contenido esencial de cada uno de los derechos. Por ejemplo, en el derecho al honor, las formas de transgresión no se limitan a la difusión de información falsa por medios de comunicación, aunque esta podría ser más dañina; es suficiente para configurarse la violación que la injuria o calumnia se hayan perpetrado con la presencia de testigos.

Finalmente, en el artículo 19, numeral 2 de la Constitución de 1978, referente al derecho a la libertad de opinión y expresión, omite la mención al derecho al honor como límite intrínseco. La norma señala que será la ley la que establezca los límites del derecho y la que instaure los casos en los que debe asignarse responsabilidad civil y penal. Además, hace expresa alusión a los representantes de medios de comunicación que no tendrán fuero especial ni inmunidad.

En la Primera Codificación de la Constitución Política de 1978, respecto del derecho al honor menciona el siguiente texto: "Artículo 19.- Sin perjuicio de otros derechos necesarios para el pleno desenvolvimiento moral y material que se deriva de la naturaleza de la persona, el Estado le garantiza: [...] 3. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar...". Este texto se asemeja al de la Constitución de 1967; es decir, se reconoce nuevamente la honra y no el honor, además la intimidad personal y familiar; dicho de otro modo, todos estos derechos indispensables para garantizar la personalidad y dignidad humana.

La única diferencia radica en la incorporación de la buena reputación que consiste en la "opinión que las gentes tienen de una persona".[81]

En esa codificación el artículo 19, numeral 4, que se refiere al derecho a la libertad de opinión y expresión incluye el texto que en la Constitución de 1978 en su versión original, acompañaba al derecho al honor, respecto del derecho de rectificación:

> Artículo 19.- Sin perjuicio de otros derechos necesarios para el pleno desenvolvimiento moral y material que se deriva de la naturaleza de la persona, el Estado le garantiza: [...] 4. El

[80] J. TOBAR DONOSO Y J. LARREA HOLGUÍN, *Derecho constitucional ecuatoriano*, 203.
[81] E. ÁLVAREZ CONDE, *Curso de Derecho constitucional*, vol. 1, 432.

> derecho a la libertad de opinión y a la expresión del pensamiento por cualquier medio de comunicación social, sin perjuicio de las responsabilidades previstas en la ley. Toda persona que fuere afectada por afirmaciones inexactas o agraviadas en su honra por publicaciones hechas por la prensa u otros medios de comunicación social, tendrá derecho a que éstos hagan la rectificación correspondiente en forma gratuita...

En la Segunda Codificación de la Constitución Política de 1978 aparece un texto exactamente igual al anterior. La Tercera Codificación de la Constitución Política de 1978, en el Título II, De Los Derechos, Deberes y Garantías, Sección I, De los Derechos de las Personas, Principios Generales señala en el "Artículo 22.- Sin perjuicio de otros derechos necesarios para el pleno desenvolvimiento moral y material que se deriva de la naturaleza de la persona, el Estado le garantiza: [...] 4. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La Ley protegerá el nombre, la imagen y la voz de la persona...". Así aparecen nuevos derechos asociados a la honra como son la imagen y la voz.

En la Cuarta Codificación de la Constitución Política de 1978, en el Título II, De los Derechos, Deberes y Garantías, Sección I, De Los Derechos de las Personas, Principios Generales, aparece el artículo 22, numeral 4, con un texto idéntico al anterior. Solo respecto del contenido del artículo 22, numeral 5, del derecho a la libertad de opinión y expresión, existe una variante relativa a que el derecho de rectificación debe ser gratuito, inmediato y proporcional.

Sobre la Constitución Política de 1998, en el Título III, De Los Derechos, Garantías y Deberes, Capítulo 2, De los derechos civiles, en el siguiente texto señala: "Artículo 23.- Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: [...] 8. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona...".

Esta misma Constitución respecto del derecho a la libertad de opinión y de expresión establece texto idéntico a su predecesora, la única variante se encuentra en el derecho a rectificar "en el mismo espacio o tiempo de la información o publicación que se rectifica" cuando ha sido afectada por afirmaciones sin pruebas o inexactas, o agraviada en su honra por informaciones o publicaciones no pagadas hechas por la prensa.

En la misma Constitución de 1998, en el Título III, De Los Derechos, Garantías y Deberes, en el Capítulo 7, De los deberes y responsabilidades, se establece por primera vez entre los deberes de los ciudadanos el de respeto a la honra ajena: "Artículo 97.- Todos los ciudadanos tendrán los siguientes deberes y responsabilidades, sin perjuicio de otros previstos en esta Constitución y la ley: [...] 5. Respetar la honra ajena".

Finalmente, en la Constitución de la República del Ecuador de 2008, en el Título II. Derechos, en el Capítulo sexto de los Derechos de libertad consta el siguiente texto: "Artículo 66.- Se reconoce y garantizará a las personas: [...] 18. El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona". En este artículo se sustituye la buena reputación por el buen nombre.

La intimidad ya no es parte del numeral 18 sino que conforma su propio numeral como derecho independiente. En la Mesa 1 de la Constituyente se pretendía añadir el siguiente texto: "sin perjuicio de las acciones penales o civiles a las que tenga derecho la persona

injuriada".[82] Asimismo otro asambleísta sostenía que "no debe hablarse de derecho al honor, lo tengo, es derecho inmanente al ser humano, más bien debemos hablar del derecho al respeto al honor de las personas, porque el honor es una condición del ser humano, por lo tanto no es derecho al honor".[83] Se mencionó también que honor "es aquel derecho que tiene toda persona, su buena imagen y nombre; de tal forma que todos tenemos derecho a que se nos respete dentro de nuestra esfera personal cualquiera que sea nuestra trayectoria, siendo un derecho único e irrenunciable, propio de todo ser humano".[84] En otras palabras, se volvió a discutir si la protección debía ser de la honra o del derecho al honor, pensando en cada uno de ellos desde una visión subjetiva u objetiva como se analizó previamente, tal como se hiciera en Constituciones anteriores, sin que dichas afirmaciones hayan tenido asidero pues la referencia constitucional final fue la del derecho al honor.

En suma, podemos reconocer el aparecimiento tardío del derecho al honor en las Constituciones ecuatorianas, al final del primer período histórico en el año 1845. En sus primeras aproximaciones constitucionales se pensaba en el honor relacionado directamente con la presunción de inocencia y no desde la percepción de la imagen de una persona en sociedad, de tal forma que la falsa atribución de un delito era la forma más visible de mancillar la buena reputación de una persona, pues ponía en tela de duda su probidad. Asimismo, la expresión delincuente en lugar de culpable evidencia una connotación no jurídica, sino más bien de estigmatización social.

En muchas ocasiones se omitió del catálogo de derechos protegidos por la Constitución y solo apareció tangencialmente como limitación a la libertad de expresión. Es decir, la honra no logra identificar elementos propios que lo ayudaran a independizarse de otros derechos, aun cuando para la transgresión no es necesaria la difusión masiva de una injuria basta con que se haya realizado frente a otra u otras personas independientemente de que sean parte de su seno familiar o no. En este conflicto de derechos entre libertad de información y derecho al honor, no es suficiente la existencia de interés público para justificar la difusión de información que atente al honor, sino que el tribunal constitucional español[85] ha señalado como elementos que permiten determinar cuándo difundir una información a los siguientes: la veracidad, ausencia de expresiones o frases formalmente injuriosas, innecesarias para la exposición de aquellas y, finalmente, la utilización de un vehículo institucionalizado de formación de la opinión pública.[86]

Es solo a partir de la Constitución de 1967 que la honra se protege como derecho autónomo e independiente sin vinculación con el principio de inocencia, como parte del debido proceso o como límite real a la libertad de opinión, aunque nuevamente en la versión original de la Constitución de 1978 se volvió a incluir una referencia a la libertad de expresión. No obstante, llama la atención como nunca ha podido constar como literal independiente, pues se la ha acompañado inicialmente de la intimidad familiar y personal (1967), de la imagen y la propia voz (1993 hasta la vigente de 2008).

Asimismo, resulta cuestionable la discusión de si el derecho a ser tutelado es la honra o el honor, incluso en los debates de la Constitución vigente, pese a que varias constituciones han

[82] ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 50], 120.
[83] Ibíd., 123.
[84] ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 64], 42.
[85] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [SSTC 105/90].
[86] T. VIDAL MARÍN, *El derecho al honor y su protección desde la Constitución Española* (Madrid: Centro de Estudios Políticos y Constitucionales y Boletín Oficial del Estado, 2000), 355.

señalado como pertinente a la honra. Suponemos que esta diferenciación proviene de la doctrina que, como vimos en su momento, utiliza los dos términos de manera distinta.

Lo importante en todo caso es concluir que el honor, desde un enfoque de afectación del espacio de lo privado e íntimo, es antecedente directo e inmediato del derecho a la protección de datos personales, tanto más que conforma junto con el conjunto de derechos que tienen por finalidad proteger el libre desarrollo de la personalidad y la salvaguarda del respeto a la dignidad humana. Se concluye también que la honra, además de ser un derecho es un límite a la libertad de expresión.

La falsa imputación de un delito sigue siendo una típica conducta transgresora de la honra; mientras que el principio de inocencia ha marcado total independencia respecto de la honra por referirse específicamente a la atribución o no de responsabilidad civil, penal o administrativa, entre otras; es decir, por su materialización en el debido proceso y en la tutela judicial efectiva.

Finalmente, el artículo 83 de la Constitución 2008 de forma general establece: "Artículo 83. Son deberes y responsabilidades de las ecuatorianas y ecuatorianos, sin perjuicio de otros previstos en la Constitución y la ley: [...] 5. Respetar los derechos humanos y luchar por su cumplimiento". Dicho de otro modo, a lo largo del texto constitucional consta reconocido un catálogo de derechos fundamentales, considerados como facultades o prerrogativas exigibles, respecto de los cuales no es suficiente el respeto o tradicional deber de abstención por parte del Estado y los particulares; sino que conforme a la norma citada, establece una dimensión positiva, por la cual, los ecuatorianos y ecuatorianas están obligados a luchar por el cumplimiento de los derechos humanos.

Esa visión significa un paso más en la defensa de los derechos en sí mismos, y en especial, por irradiación, de todo el bloque de derechos que protege la dignidad humana desde el enfoque de la defensa del proceso de autoconstrucción de la persona en sociedad.

2.5 Derecho a la intimidad (1967)

El derecho a la intimidad carece de antecedentes en los criterios jurídicos griegos y romanos, "el sentido de la intimidad misma, del ámbito de las relaciones personales como algo sagrado por derecho propio, se deriva de una concepción de la libertad que, a pesar de sus orígenes religiosos, en su estado desarrollado apenas es más antigua que el Renacimiento o la reforma".[87] Si bien, "la intimidad ha sido una necesidad desde tiempo inmemorables de la humanidad, ya que también se puede tratar de un instinto de supervivencia; pero no siempre se deslindó jurídicamente hablando, correctamente la realidad de la intimidad respecto al ámbito del honor con el que aparecía de algún modo vinculado en sus inicios".[88]

El derecho a la intimidad aparece como respuesta a las necesidades de la naciente burguesía que anhelaba para sí un derecho atribuido hasta entonces a los nobles, quienes cumplían con la condición de propietarios y por ende eran aquellos que podían acceder a espacios de intimidad.[89] Si bien coincide con la consagración de los "derechos del hombre, no supuso en

[87] I. BERLÍN, *Cuatro ensayos sobre la libertad*, 229.
[88] M. A. ENCABO VERA, *Derechos de la personalidad*, 101.
[89] A.M. BENDICH, *Privacy, Poverty and the Constitution, en vol. Conference on the Law of the poor* (Berkeley: University of California, Berkeley, 1966), 7. ‹http://links.jstor.org/sici?sici=0008-1221(196605)54%3A2%3C407%3APPATC%3E2.0.CO%3B2-9›. Consulta: 16 de junio de 2007.

la sociedad burguesa la realización de una exigencia natural de todos los hombres, sino la consagración de privilegio de una clase".[90] Entonces, la intimidad fue considerada un privilegio de clase en la Revolución Industrial.

Posteriormente, la intimidad fue reconocida a partir de 1948, cuando la Declaración Universal de los Derechos Humanos la recoge en el artículo 12 y señala que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Este texto ha sido reproducido casi íntegramente por el artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos de Naciones Unidas.

Asimismo, el Convenio Europeo de los Derechos Humanos y de las Libertades Fundamentales, celebrado en Roma, el 4 de noviembre de 1950, recoge norma similar que dice:

> Artículo 8.- Derecho al respeto a la vida privada y familiar. 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

El convenio menciona las posibles excepciones que pueden justificar una intromisión en la vida privada, familiar, su domicilio y correspondencia, siempre y cuando tengan motivo suficiente que las justifiquen y se encuentren específicamente determinadas en la ley.

En Ecuador, el derecho a la intimidad fue incorporado como derecho a partir de la Constitución de 1967; es decir, aparece en el tercer período republicano —el proyecto nacional de la diversidad— marcado por profundos cambios económicos, políticos, sociales e incluso en la forma de adquirir conocimiento y en el desarrollo de la ciencia y la tecnología; además acompañado de una larga crisis económica.

Con la finalidad de identificar los motivos que tuvieron los constituyentes para incluir este nuevo derecho, se realizó una investigación directa en las 233 actas de debate de la Comisión de la Constitución; así como en las 53 actas del año 1966 y 118 actas del año 1967 de sesiones ordinarias y extraordinarias de la Asamblea Constituyente que constan en el Archivo Biblioteca de la Función Legislativa.[91]

La versión original del numeral 4 del artículo 27, presentada por la Comisión, era la siguiente: "4. El derecho a la intimidad y a una eficaz protección contra los ataques a su honra o a su vida privada".[92] Las discusiones se plantearon respecto al "contenido estricto de la palabra intimidad". El honorable Salazar Alvarado solicitó que se redactara de otra forma el mencionado artículo, pues consideraba que:

---

[90] S. RODOTA, *La privacy tra individuo e collettivitá*. ‹http://www.emsf.rai.it/grillo/trasmissioni.asp?d=607›. Consulta: 16 de junio de 2007.

[91] La investigación se realizó respecto de la totalidad de las actas debido a que la información consta únicamente en versión física y no ha sido sometida a una sistematización, por lo que no se encuentra indexada por temas.

[92] ASAMBLEA NACIONAL CONSTITUYENTE DE 1967 DE ECUADOR, [Acta No. 46], 35.

> [...] ciertamente la palabra intimidad no corresponde a aquello que se está queriendo decir aquí. No pediría sino revisar el Diccionario de la Real Academia de la Lengua para que se vea que esa palabra tiene otro sentido distinto. En cambio, si se habla de la intimidad de la vida privada, bastará esta redacción, que concuerda con la redacción del artículo 12 de la Declaración de los Derechos del Hombre.[93]

Como vemos, se proponía eliminar la referencia a la intimidad. Puesto que se consideraba pertinente mantener una redacción conforme al artículo 12 de la Declaración de los Derechos del Hombre, antes citada, que establecía como derecho la prohibición de injerencias o ataques arbitrarios a los espacios de privacidad de un individuo como son la familia, el domicilio o la correspondencia sin que en la norma se mencione el término intimidad.

Al respecto, la intimidad es un concepto jurídico contemporáneo que aparece en 1890 de una publicación realizada por Charless Warren y Lois Brandeis, quienes publicaron la obra *The Right to Privacy*, que ante la falta de un término exacto se traduce en derecho a la intimidad. Se conceptualiza como el derecho a *estar solo*; o "el derecho a disfrutar de determinadas zonas de retiro y secreto de las que podemos excluir a los demás";[94] o el ámbito o reducto intransferible de la soledad[95] "en el que se veda que otros penetren";[96] o de un "ámbito propio y reservado frente a la acción y conocimiento de los demás".[97] De tal forma que se protege la vida privada o íntima de la persona. Los alemanes, en varias sentencias de sus tribunales, postularon un sistema de identificación del ámbito de la intimidad, al que denominaron teoría de las esferas, por las cuales, tenían mayor a menor rango de protección según se viabilizaba o no la injerencia de terceros en tales espacios. La primera, la esfera íntima; la segunda, la esfera privada; y la tercera, la esfera de lo individual, social o pública. No obstante, esta teoría de las esferas fue paulatinamente superada por la doctrina principalmente por la "dificultad —por no decir imposibilidad— de trazar unas fronteras nítidas entre las diversas esferas".[98]

Varios autores sostienen que vida privada e intimidad no pueden ser usadas como sinónimos ya que la primera abarcaría situaciones que no podrían ser determinadas como íntimas.[99] "Así, por ejemplo, la práctica de deportes en un club de fin de semana no sería algo íntimo, pero sí de la vida privada".[100] Por su parte, otros autores hablan del reconocimiento de un "espacio vital propio" dentro del que puede moverse cada persona, de tal forma que se distingue "entre esfera secreta (Geheimsphare), que se traduce en el secreto de

---

[93] Ibíd.
[94] M. CARRASCO DURÁN Y J. PÉREZ ROYO, *Curso de derecho constitucional*, 293.
[95] S. E. CIFUENTES, *Derechos personalísimos*, 582.
[96] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 73/1982].
[97] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 57/1984].
[98] M. MEDINA GUERRERO, *La protección constitucional de la intimidad frente a los medios de comunicación* (Valencia: Tirant lo Blanch, 2005, 18).
[99] Carlos Santiago Nino manifiesta: "La intimidad de una persona, o sea la exclusión potencial de acuerdo a su voluntad del conocimiento y la intrusión de los demás, se refiere al menos a los siguientes aspectos: rasgos de su cuerpo, su imagen (la que, no obstante la inevitabilidad de su percepción por los demás en la vida cotidiana, la persona puede querer que no se produzca, sobre todo en ciertas circunstancias), pensamientos y emociones, circunstancias vividas y diversos hechos pasados conectados con su vida o la de su familia, conductas de la persona que no tengan una dimensión intersubjetiva, escritos, pinturas, grabaciones hechas por la persona en cuestión, conversaciones con otros en forma directa o por medios técnicos (como el teléfono), la correspondencia, objetos de uso persona, su domicilio, datos sobre su situación económica, etcétera". Ver C. S. NINO, *Fundamentos de derecho constitucional: análisis filosófico, jurídico y politológico de la práctica constitucional* (Buenos Aires: Editorial Astrea De A. y R. DePalma, 1992), 328.
[100] S. E. CIFUENTES, *Derechos personalísimos*, 618.

correspondencia, un derecho al respeto de la esfera privada (Privatsphare) y un derecho a la integridad de la vida íntima espiritual".[101]

Si bien, no existe uniformidad sobre varios elementos que materializan o caracterizan el derecho a la intimidad, sin embargo su núcleo esencial no ha cambiado aunque se han incluido varias manifestaciones con base a este derecho.[102] La mayoría de la doctrina y de la normativa señala que las transgresiones a la intimidad se presentan desde la perspectiva de las intromisiones ilegítimas, culposas o dolosas, que no están autorizadas o consentidas y que han sido realizadas por parte de medios de comunicación, que se dedicaban a esculcar la vida de las personas y a publicarla para conocimiento de todos, de una autoridad o de cualquier persona que pueden usar la información con otras finalidades. En este sentido, se ha señalado que "la solución exige determinar el límite entre el legítimo ejercicio del derecho de crónica y de crítica, por una parte, y la indebida invasión de la esfera ajena, por otra".[103]

Se configura la transgresión a la intimidad, si es que se accede[104] o se divulga[105] información sobre la vida privada o íntima, cuando no existe consentimiento expreso, ya sea por su falta o por su negativa. El consentimiento es revocable en cualquier momento. Así, en este elemento radica su diferencia con el honor, que se afecta únicamente si las imputaciones son falsas.

No es indispensable que el acceso o la divulgación se produzcan simultáneamente, basta con la configuración de uno de ellos para que exista violación a la intimidad. Incluso si se obtuvo la información de forma lícita es indispensable el consentimiento para su difusión. La intimidad protege la corporeidad, ya que el cuerpo es el soporte del derecho de la propia imagen y también de la intimidad. Asimismo, está incluida la intimidad informativa, de tal forma que protege a la persona de la intromisión, independientemente de que haya causado daño su difusión. En consecuencia, la intimidad informativa consiste en el derecho a poder determinar, por nosotros mismos, cuándo, cómo y con qué alcance se va a transmitir información sobre nosotros a los demás.[106] Actualmente la intimidad no es solo una "facultad

---

[101] L. ENNECCERUS Y H. C. NIPPERDEY, Derecho civil (Parte general), t. I. Trad. por B. Pérez González y J. Alguer, Barcelona, 1943, citado por A. VALENCIA ZEA, *Derecho civil*, vol. I, 388.

[102] "El Tribunal Supremo, en Roe vs. Wade reconoció el derecho constitucional de la mujer embarazada a interrumpir el embarazo. Se trata de la «decisión más íntima y personal» que puede tomar un ser humano y en la cual no pueden interferir ni los poderes públicos ni los demás ciudadanos". M. CARRASCO DURÁN Y J. PÉREZ ROYO, *Curso de derecho constitucional*, 293.

[103] A. ALESSANDRI RODRÍGUEZ Y OTROS, *Tratado de derecho civil*, 490.

[104] "El acceso o la obtención de información que produce intromisiones ilegítimas se realiza a través de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción. Se incluye la cámara oculta en los reportajes periodísticos. No solo imágenes obtenidas en un ámbito o entrone doméstico o privado sino incluso a las imágenes obtenidas de forma clandestina en lugares públicos". M. CARRASCO DURÁN Y J. PÉREZ ROYO, *Curso de derecho constitucional*, 294.

[105] Se incluye aquella información que es conocida mediante actividades profesionales, y es oficial de quien la revela por haber sido desviada del fin para el cual se suministró inicialmente. Su uso se convierte en una intromisión ilegítima. Ibíd., 295.

[106] Ibíd. Por cuanto es difícil determinar los ámbitos que deben quedar protegidos por el derecho a la intimidad o privacidad personal y familiar, usualmente se acude a los tribunales de derechos humamos. El Tribunal de Estrasburgo en esta materia (TEDH) "defiende una concepción ampliar de lo que debe ser protegido: el respeto de la vida privada debe también englobar hasta cierto punto el derecho a establecer y desarrollar relaciones con otros seres humanos (sentencia de 16 diciembre de 1992, Caso Niemietz contra Alemania), que comprende actividades como las relativas a la vida e identidad sexuales (26 de marzo 85, X e Y contra los Países Bajos), la confidencialidad de datos sobre salud (25 de febrero 1997, Z. contra Finlandia), la elección del propio nombre (22 de febrero de 1994, Burghatsz contra Suiza), la defensa de la familia frente a la expulsión del territorio de un

de aislamiento implica un derecho de participación y de control en las informaciones que conciernen a cada persona".[107]

De producirse el reconocimiento judicial de una transgresión a la intimidad, se procederá con la indemnización de los daños y perjuicios causados, incluyendo en ellos las expectativas justificadas.

Finalmente, se vuelve necesario establecer los casos en que las intromisiones son legítimas; dicho de otro modo, cuándo los poderes públicos pueden justificar límites al derecho a la intimidad personal y familiar. Al respecto, la jurisprudencia constitucional española[108] ha venido aplicando el habitual canon de constitucionalidad de las medidas:[109] a) las restricciones deberán venir amparadas por ley (por ejemplo cuando la conducta íntima ofenda el orden público, la moral pública o perjudique a otras personas o se habilite la transgresión en atención a razones de interés general por considerarse de carácter histórico, científico o cultural);[110] b) cuando la finalidad sea legítima;[111] c) sean adoptadas por autoridad judicial, o administrativa siempre y cuando exista previa habilitación legal; d) sean motivadas y conforme a criterios de proporcionalidad en sentido amplio[112] (idoneidad, necesidad y proporcionalidad en sentido estricto);[113] y, en conflicto con el derecho a la libertad de información, prima este siempre y cuando se configuren dos presupuestos: la relevancia pública de la información y la veracidad de la información transmitida.[114]

Luego de esta breve revisión doctrinaria y jurisprudencial podemos analizar la intervención del honorable Julio César Trujillo, con la finalidad de verificar si su contenido se alinea con el desarrollo de este derecho en otras latitudes. Al respecto, el mencionado honorable en defensa de la intimidad, en los debates constitucionales señaló:

> [...] tenemos que reconocer que hay un ámbito de la vida del individuo, dentro del cual no tiene competencia alguna el Estado, dicho ámbito aparte de la vida privada de él, comprende una serie de concepciones de la vida, comprende actitudes ante ella, y además, una serie de decisiones sobre las cuales el Estado no tiene ninguna competencia, ni podemos reconocerla. Hay, pues, un ámbito de la vida dentro del cual el Estado, repito, no tiene ninguna competencia. En este sentido está tomado el término intimidad. La vida privada comprende una extensión un tanto más amplia y comprende todas las actividades del individuo, en orden a su vida particular. Así, por ejemplo, no parece lícito que se pueda aprovechar ciertas

---

ciudadano extranjero (2 de agosto de 2001, Boultif contra Suiza), o la protección frente a intromisiones nocivas y molestas de ruidos y olores en los espacios en los que se desarrolla la vida privada (9 de diciembre de1995, López Ostra contra España). Esta última línea ha sido recogida por el Tribunal Constitucional, tradicionalmente algo más auto al respecto, en la STC 119/2001, en que admite la posibilidad de entender como intromisión ilegítima la contaminación acústica en la medida que sus efectos impida o dificulten gravemente el libre desarrollo de la personalidad". Ibíd.

[107] A. E. PÉREZ LUÑO, *Derechos humanos, estado de derecho y Constitución*, 7a. ed. (Madrid: Tecnos, 2001, 333.

[108] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 134/1999].

[109] M. APARICIO PÉREZ; M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 703. "Su aplicación deberá ser ponderada caso por caso en el ámbito judicial, aunque tratándose de limitaciones de derechos fundamentales la concurrencia de tales intereses deberá ser interpretada restrictivamente". Ibíd., 700.

[110] M. CARRASCO DURÁN; J. PÉREZ ROYO, *Curso de derecho constitucional*, 295.

[111] S. E. CIFUENTES, *Derechos personalísimos*, 594. Véase J. RIVERA, *Instituciones del Derecho Civil*, vol. II (Buenos Aires: Abeledo Perrot, 1992), 79.

[112] Se autoriza la intromisión para las investigaciones de delitos, una adecuada determinación que permita el cobro de tributos, la prueba de paternidad o maternidad contra la voluntad del sujeto afectado.

[113] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 702.

[114] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 139/2007].

> declaraciones y actuaciones del individuo en su vida privada, con algún fin. Es muy frecuente, desgraciadamente, en el mundo actual el uso de documentos incluso de fotografías que revelan situaciones de la vida privada del individuo; las que se pueden hacer en el seno de la intimidad, que se utilizan no solo con fines políticos sino aún con fines de lucro y de menoscabo de la dignidad de la persona humana. En este sentido está tomada la palabra intimidad en este artículo[115] [...] (intimidad) revela un cambio en la vida del hombre, campo que es distinto, mucho más profundo que el de la vida privada".[116]

De la transcripción se desprende que era propuesta del legislador Trujillo incluir a la intimidad como derecho. Por lo tanto, el término no era un equívoco idiomático que debía evitarse manteniéndose la redacción que hacía alusión exclusivamente a las injerencias arbitrarias a la vida privada señalada en la Declaración de Derechos Humanos, conforme argumentó el honorable Salazar Alvarado.

Al contrario, de la argumentación presentada por el honorable Trujillo se visibiliza el contenido esencial del derecho a la intimidad. Esto es la clara diferenciación entre vida privada e intimidad, determinando que el derecho no debe limitarse a la protección de la primera, que solo se refiere a las actividades del individuo en su vida particular, sino que debe garantizarse un ámbito más profundo de protección relativo a la *serie de concepciones de la vida, actitudes ante ella, decisiones sobre las cuales el Estado no tiene ninguna competencia*.[117]

El legislador aclara con vehemencia que, respecto de este espacio íntimo y de las decisiones que las personas tomen dentro de él, no tiene injerencia o competencia alguna el Estado. Esta afirmación visibiliza al Estado como el principal y potencial transgresor. En conclusión, se justifica la necesidad de incorporar a la intimidad en el catálogo de derechos, debido a que es necesario garantizar que la información íntima no pueda ser usada con fines políticos, lucrativos o de *menoscabo de la dignidad de la persona humana*. En el mismo sentido, el Honorable Villacrés por su parte arguyó:

> La indicación del Honorable Salazar Alvarado viene a distorsionar totalmente el concepto establecido en el numeral 4°. En realidad, si se aceptase su indicación, tendríamos que concluir que solo se desecha lo arbitrario y se acepta lo que no es arbitrario, lo cual desnaturaliza totalmente la garantía que se establece en el numeral 4. En segundo lugar, se trata de establecer un nuevo derecho, y es aquel, de que el individuo esté garantizado en su vida personal y familiar, que lo considera íntima, no puede ser objeto de publicidad ni de conocimiento público. Para todos es conocido que se han hecho inventos por medio de los cuales actualmente ni la conversación entre dos personas puede ser reservada, porque los adelantos técnicos pueden grabar la conversación privada. Entonces, nosotros tenemos que adelantarnos en estas innovaciones y establecer esta garantía. Así mismo, es conocido que se publican fotografías que resultan inconvenientes para la persona en su vida privada y particular. Contra todo esto se está garantizando en este numeral. De manera que es un nuevo derecho que los señores Juristas lo consignaron en su proyecto".[118]

Villacrés expresamente señala que no se puede recoger el texto de la Declaración Universal de los Derechos del Hombre, pues la intención del constituyente es incorporar un nuevo derecho cuyo contenido pretende evitar que información *personal y familiar e íntima pueda*

[115] ASAMBLEA NACIONAL CONSTITUYENTE DE 1967 DE ECUADOR, [Acta No. 46], 34.
[116] Ibíd., 36.
[117] Ibíd.
[118] Ibíd., 35.

ser objeto de publicidad o conocimiento público. Llama la atención que la justificación se realiza desde los nuevos instrumentos tecnológicos que permiten registrar eventos privados que pueden luego divulgarse perjudicando a sus titulares. Si bien, en otras latitudes se justifica la incorporación de este derecho como limitación a la libertad de prensa; no obstante, la propuesta ecuatoriana se decanta de posibles transgresiones estatales o particulares con afán de lucro, en la cual también, pero no únicamente, se incluye a la prensa.

De otro lado, el honorable Levi Castillo proponía que el artículo incorpore una frase final que diga "inviolabilidad de domicilio en todo el tiempo". Y para ello argumentaba lo siguiente: "El derecho a la intimidad es del hogar, pero esa intimidad fue muchas veces violada en tiempo de la dictadura y en tiempos pos constitucionales también se ha violado domicilios (sic), se ha sacado de ellos cosas, muebles, etc. incluso personas que han estado dentro de los domicilios". Los constituyentes consideraron impertinente este texto, ya que la inviolabilidad del domicilio se encuentra reconocida en otro numeral del mencionado artículo 28. Sin embargo, es materia de análisis la asociación de la intimidad con el hogar y a la inviolabilidad del domicilio como derecho instrumental que también garantizaría a la intimidad.

Luego de la revisión gramatical por parte de los especialistas, y atendiendo a la aclaración de que en el artículo 28 reconocen dos derechos independientes, el texto final del numeral 4 del artículo 28, contenido en el Capítulo II, en el título De los Derechos de la Persona, señala: "Derechos garantizados.- Sin perjuicio de otros derechos que se deriven de la naturaleza de la persona, el Estado le garantiza: [...] 4. El derecho a la honra y a la intimidad personal y familiar". Esta clara y simple redacción elimina la frase que hacía alusión que a través de la intimidad se lograba una "eficaz protección contra los ataques a la honra y a la vida privada". A la intimidad no solo se la transgrede cuando hay difusión de información íntima, familiar o privada, sino que, como se señaló en líneas anteriores, basta con el simple acceso para que se configure la transgresión al derecho; además que no solo establece un deber de abstención con efecto *erga omnes*, sino que permite al titular su autodeterminación informativa. Mientras que la honra se quebranta con una falsa atribución que es difamante o calumniosa. De tal suerte, que si una atribución de un aspecto íntimo o privado de la persona resultare verdadero no existe transgresión al derecho al honor, sino al derecho a la intimidad.

Acerca de la Constitución de 1978, en su versión original elimina el derecho a la intimidad. El motivo de esta supresión es la decisión de la Asamblea Constituyente de realizar una breve mención de los derechos de las personas, pues consideraban que estos se hallan inmersos en la Declaración Universal de Derechos Humanos, de la que Ecuador es parte. Asimismo, consideraban que no debían constar en artículos ni capítulos distintos los derechos civiles y políticos de los económicos y sociales, sino que "todos son derechos humanos que toda democracia debe garantizar".[119]

Las reformas a la Constitución, promulgadas en los Registros Oficiales 180, de 5 de mayo de 1980 y 169, de 1 de septiembre de 1983, viabilizan la Primera Codificación de la Constitución Política de 1978, mediante la cual se vuelve a incluir el derecho a la intimidad con el siguiente texto: "Título II, De los Derechos, Deberes y Garantías, Sección I, De Los Derechos de la Persona: "Artículo 19.- Sin perjuicio de otros derechos necesarios para el pleno desenvolvimiento moral y material que se deriva de la naturaleza de la persona, el

[119] ASAMBLEA NACIONAL CONSTITUYENTE DE 1977 DE ECUADOR, [Acta No. 30], 3.

Estado le garantiza: [...] 3. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar".

Desaparece la alusión equívoca a la libertad de expresión que constaba en la versión original de la Constitución de 1978 y se recupera el texto de la Constitución de 1967 con un añadido que hace referencia a la "buena reputación". En la Segunda Codificación de la Constitución Política de 1978 consta el mismo texto.

La Constitución Política de 1978, en su Tercera Codificación, añade que "La Ley protegerá el nombre, la imagen y la voz de la persona". Sobre este nuevo derecho se analizará en el siguiente subtítulo del presente trabajo. Igual norma constitucional, incluido el derecho añadido se repite en la Cuarta Codificación de la Constitución Política de 1978.

Respecto de la Constitución Política de 1998, en el Título III, De Los Derechos, Garantías y Deberes, Capítulo 2, De los derechos civiles, consta una versión del derecho, idéntica a su predecesora. Fue aprobada sin observaciones[120] y el texto es el siguiente: "Artículo 23.- Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: [...] 8. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona".

Finalmente, en la Constitución de la República del Ecuador de 2008, en el Título II, Derechos, Capítulo segundo, Derechos del buen vivir, Capítulo sexto, Derechos de libertad consta el siguiente texto: "Artículo 66.- Se reconoce y garantizará a las personas: [...] 20. El derecho a la intimidad personal y familiar". Esta es la primera vez que una Constitución ecuatoriana reconoce este derecho como autónomo, de tal forma que lo consagra en la estructura de la norma en un numeral independiente.

En el primer debate del texto constitucional del 2008 se realizó el siguiente análisis: "La intimidad es la parte interior que solamente cada uno conoce de sí mismo, es el máximo grado de inmanencia, es decir aquello que se almacena en el interior. Lo íntimo está protegido por el sentimiento de pudor. Por su parte, en la expresión de intimidad, se coloca en juego la capacidad de dar y la posibilidad de dialogar con otra intimidad diferente. La dignidad humana dentro de la esfera de lo social se garantiza en la medida en que se tenga la posibilidad de conservar su privacidad, entendida, como aquel fuero interno que solo puede interesar al ser humano como individuo o dentro de un contexto reducido de personas que en últimas, está determinado por el consentimiento de quien es depositario de su existencia. El Diccionario de la Real Academia define intimidad como zona espiritual e íntima y reservada de una persona o de un grupo, especialmente, de una familia. Esta zona reservada de la persona humana y de la familia, la protege en forma clara el artículo citado, al prescribir que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre y el Estado debe respetarlos y hacerlos respetar".

Del texto transcrito, se puede concluir que la norma constitucional contempla el derecho a la intimidad, desde su sentido más simple; es decir, la protección de la información personal, *sobre sí mismo,* y también de la relativa "a la intimidad familiar por ser una zona espiritual, íntima y reservada de un núcleo",[121] conforme se señaló en el segundo debate de la

[120] ASAMBLEA NACIONAL CONSTITUYENTE DE 1998 DE ECUADOR, [Acta No. 46], 49; [Acta No. 80], 15.
[121] ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 64], 42.

Constitución de 2008. En otras palabras, no se hace referencia a la privacidad *como el derecho a estar solo*; es decir, como el derecho a exigir respeto sobre su privacidad ante cualquier tipo de injerencia o intromisión ilegítima por parte de un tercero no autorizado o respecto de la divulgación de datos privados o íntimos en transgresión a la confianza otorgada. Cabe esta aclaración, debido a que la visión reduccionista, que considera que el derecho a la intimidad solo se aplica en espacios domésticos o privados, afecta la vigencia del derecho que también puede transgredirse en espacios públicos[122] e incluso respecto de personajes notorios, quienes conservan en sus relaciones personales, aún espacios de privacidad e intimidad. El Tribunal Europeo de Derechos Humanos ha señalado que existe una zona de interacción entre el individuo y los demás que, incluso en un contexto público, puede formar parte de la vida privada.[123] Este derecho al igual que todos no es absoluto, también puede ser sometido a límites tanto inmanentes como requisitos de veracidad y de interés general o de relevancia pública de la información (SSTC 68/2008, FJ 3; y 129/2009, de 1 de junio, FJ 27 2); así como límites externos como el derecho a la información.

En conclusión, la protección del derecho a la intimidad se reconoce en Ecuador con posterioridad a la Declaratoria de Derechos Humanos, no como un derecho de clase desde la óptica europea, tampoco desde su debate con la libertad de expresión desde la visión norteamericana, sino que llega a esta latitud de la mano del desarrollo tecnológico, producto de los avances científicos y de los medios de difusión masiva de la información. Si bien, su precedente directo está en el artículo 12 de la Declaración de Derechos Humanos, norma que se incorpora paulatinamente en los textos constitucionales latinoamericanos, tuvo en la motivación de los constituyentes ecuatorianos elementos definidores sobre la protección de los ciudadanos respecto de las persecuciones estatales y del abuso de los particulares, incluidos los medios de comunicación, que se lucran de la intimidad de sus ciudadanos.

La incorporación de la intimidad como derecho de principal protección, entre los derechos de la personalidad, se produce a partir de evitar transgresiones al ejercicio de libertades individuales, de propender al libre desarrollo de la personalidad y al respeto a la dignidad humana, todos ellos elementos comunes e indispensables para mantener una mínima calidad de vida[124] desde la perspectiva del hombre en su entorno social.

De ahí que en el actual texto constitucional la intimidad se constituye como un derecho autónomo y diferenciado de otros como el honor, la inviolabilidad de domicilio, correspondencia e incluso del naciente derecho de protección de datos personales. De este último, si bien es antecedente inmediato y directo, ha logrado separarse. Intimidad y protección de datos personales constituyen derechos emancipados y suficientes que deben ser garantizados por el Estado desde distintas ópticas, no solo imponiendo deberes de abstención como en el caso de la intimidad sino obligaciones y deberes de cuidado como en el caso de la protección de datos personales, y en ambos casos estableciendo la visión positiva del derecho a la autodeterminación informativa de una persona. Ahora bien, los dos derechos en conjunto confluyen para garantizar un espacio suficiente de protección de la persona en su interrelación con otros en sociedad.

2.6 Derecho a la imagen y a la voz (1996)

[122] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 12/2012], FJ 5.
[123] GRAN SALA DEL TRIBUNAL CONSTITUCIONAL ALEMÁN, [Sentencia Von Hannover c. Alemania], § 95.
[124] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 231/1988].

Los incesantes avances tecnológicos, que se potencian día tras día, ya no solo se manifiestan en la recolección y manipulación de imágenes y voz de las personas que manifiestamente ponen en riesgo varios derechos de las personas como la honra, la intimidad, la protección de datos personales. Se vuelve fundamental que el derecho responda a las necesidades actuales con rapidez, versatilidad y creatividad, mediante el desarrollo de los contenidos, significados, ámbitos, alcances y formas de aplicación de este conjunto de derechos que protege la interrelación de la persona, no solo en el entorno real sino especialmente en el digital.

A continuación se realizará un análisis histórico, normativo y constitucional que de manera cronológica describe cómo se ha abordado la imagen y la voz en Ecuador hasta su vigente manifestación en la Constitución de 2008.[125]

2.6.1 Antecedentes y naturaleza jurídica de los derechos a la imagen y la voz de la persona

Por ser de reciente aparición era muy común la confusión de los derechos a la imagen y a la voz con alguno de los otros bienes personalísimos.[126] Cifuentes señala el desarrollo histórico de este derecho en siete diferentes teorías. En un primer momento, se asimilaba la "imagen como una manifestación del cuerpo; luego, del mismo modo que el individuo tiene derecho a su propio cuerpo, debe tenerlo a la propia imagen".[127] En una segunda teoría se consideraba "emanación de la personalidad; no es el cuerpo el objeto del derecho, sino la figura exteriorizada en los rasgos físicos",[128] y por tanto, la trasgresión se configura desde la intromisión a la autonomía individual.

En la tercera teoría, liderada por Enneccerus, que fuera apoyada por autores como Coviello, De Oliva, De Castro, entre otros, se niega la existencia de un derecho propio bajo la premisa de que "no puede prohibirse la impresión en la mente de la imagen de una persona, así tampoco puede negarse la exteriorización de la misma",[129] de tal manera que, en una cuarta versión más depurada, señala que la única forma de proteger la imagen es desde la tutela al honor.

En una quinta propuesta se consideraba a la intimidad entrelazada con la propia imagen, de tal forma que, si bien es solo una de sus manifestaciones, logra alcanzar su autonomía debido a los adelantos técnicos ya que su transgresión se realiza con facilidad y frecuencia Por su parte, Lacruz considera que "para hacer pública la reproducción gráfica de cualquier persona, mediante cualquier proceso técnico de reproducción, es necesario contar con consentimiento".[130]

La sexta teoría relaciona la imagen con el derecho de propiedad desde la perspectiva patrimonial, material y moral. Finamente, la séptima teoría, sostenida por Rietschel, considera a la imagen como parte de la identidad personal.[131]

[125] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR [2008].
[126] S. E. CIFUENTES, *Derechos personalísimos,* 542.
[127] Ibíd., 543.
[128] Ibíd.
[129] Ibíd., 544.
[130] C. LASARTE ÁLVAREZ, *Principios de derecho civil*, t. I (Madrid: Marcial Pons, 2016), 161.
[131] S. E. CIFUENTES, *Derechos personalísimos,* 545.

Sin embargo, la realidad de las formas de transgresión del derecho a la imagen ha permitido que se reconozca como derecho propio, ya que su acaecimiento no significa violación a la propiedad, a la identidad, al honor o a la intimidad. Por ejemplo, la reproducción de la imagen de una persona sin su autorización puede producirse sin que esta suponga lesión a su buen nombre o a su vida íntima.[132]

Además, la imagen no es elemento de la identidad, como señaló en su momento Morales citado por Cifuentes, para quien nace de un interés preponderante de la persona de individualizarse en un entorno y no de la simple identificación personal que, en cambio, tiene su origen en el interés social de reconocer al individuo tal cual es.[133]

La imagen es parte del derecho a la personalidad que, desde la autodeterminación informativa, garantiza el libre desarrollo de la personalidad desde el "ámbito de libertad de una persona respecto de los atributos más característicos, propios e inmediatos como son la imagen física, la voz o el nombre, cualidades definitorias del ser propio y atribuidas como posesión inherente e irreductible a toda persona".[134]

En consecuencia, se configura como un derecho autónomo, si bien derivado de la dignidad y conexo con el honor, la intimidad, entre otros, pero referido específicamente a la captación, reproducción, publicación y difusión de la imagen y la voz, e incluso en varias legislaciones como la española del nombre de la persona.[135]

De ese modo, el derecho a la propia imagen salvaguarda un ámbito privado aunque no íntimo, pues permite el libre desarrollo de la propia personalidad para a un tercero autorizar o no y en qué dimensión la obtención, reproducción, publicación o difusión que le pueda hacer identificable o reconocible, de su información gráfica generada por sus rasgos físicos, facciones, la figura o silueta de una persona, por cualquier medio como una fotografía, filme, dibujo, grabado, caricaturas, obra de arte figurativa, entre otros, ya sea que la finalidad sea informativa, comercial, científica, cultural, etc. Sobre la identificabilidad de una representación, el afectado deberá demostrar que la exteriorización de aquellas manifestaciones es reconocible en su persona.[136]

En lo que respecta a la captación y reproducción de la imagen física de la persona y de la voz solo las personas físicas, cualquiera sea su edad, condición o nacionalidad, pueden ser titulares del derecho.[137] No son titulares de este derecho las personas ideales por carecer de existencia corporal, de una figura, fisonomía o de naturales signos somáticos.[138]

De nuevo el consentimiento se erige como aspecto central del derecho: si hay consentimiento no hay vulneración. Y en virtud de la autodeterminación informativa el consentimiento debe ser expreso y revocable en cualquier momento. Ahora bien, como también sucede en el ámbito de la intimidad, la Ley orgánica 1/1982 precisa que en caso de revocación del

[132] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 81/2001].
[133] S. E. CIFUENTES, *Derechos personalísimos,* 547.
[134] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 117/1994], FJ 3.
[135] Artículo 7 numeral 6 de la LEY ORGÁNICA 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen de España.
[136] M. A. ENCABO VERA, *Derechos de la personalidad,* 126.
[137] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 81/2001].
[138] A. M. ROMERO COLOMA, *Los bienes y derechos de la personalidad* (Madrid: Trivium, 1985), 80.

consentimiento habrán de indemnizarse, en su caso, los daños y perjuicios causados, incluyendo en ellos las expectativas justificadas (artículo 2.3).[139]

También se diferencia la protección del derecho al nombre, la imagen y la voz como manifestación de libertad individual, de los valores comerciales, económicos o patrimoniales que producen estos derechos, por lo que en este ámbito su regulación será civil.[140] Así, "el derecho fundamental a la propia imagen es diferente del derecho a la explotación comercial de la misma, aunque en determinadas circunstancias pueda ocurrir que la explotación inconsentida de la imagen de una persona pueda afectar al derecho fundamental".[141]

Cuando se conceptualiza a la imagen como derecho autónomo e independiente se establecen excepciones justificadas en la necesidad de preservar otros derechos o bienes constitucionalmente protegidos. Por consiguiente, en la mayoría de las legislaciones se autoriza la difusión de imágenes de personas ausentes, desaparecidas o imputadas en procesos penales con orden de captura. Asimismo, es posible la captación, reproducción o publicación de las representaciones gráficas, incluidas las caricaturas, de quienes ostenten un cargo o una profesión pública.[142]

El artículo 8, numerales 1 y 2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, señala los casos en que "no se reputará, con carácter general, intromisiones ilegítimas" para la obtención de imágenes de las personas: a) cuando la Autoridad competente de acuerdo con la ley lo haya autorizado o acordado; b) cuando predomina un interés histórico, científico o cultural relevante; c) cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público; excepto cuando las autoridades desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza; d) cuando se utilice la caricatura de acuerdo con el uso social; y, e) cuando la imagen de una persona determinada aparezca como meramente accesoria.

2.6.2 Los derechos a la imagen y a la voz de la persona en Ecuador

Los derechos a la imagen y a la voz de la persona aparecen por primera vez en las reformas constitucionales presentadas por el Presidente de la República, el 4 de octubre de 1994, que tratan de los temas absueltos por el pueblo ecuatoriano en la Consulta Popular de 28 de agosto de 1994 y otras presentadas en el mismo pedido de reformas.

En la versión presentada por el ejecutivo, a continuación del numeral 8 del artículo 23 de la Constitución que se refería al derecho a la honra, a la buena reputación y a la intimidad personal y familiar, se proponía incluir el siguiente texto: "sin que se pueda usar arbitrariamente la imagen y la voz de una persona para agraviarle o causarle perjuicio".[143] Dicho de otra manera, el contenido del derecho estaba atado al honor; por lo tanto, la propuesta se basaba en las primeras formas de conceptualización del derecho como manifestaciones pragmáticas de transgresiones al buen nombre.

---

[139] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 704.
[140] Ibíd., 705.
[141] A. GARRIGA DOMÍNGUEZ, *Nuevos retos para la protección de datos personales: en la Era del Big Data y de la computación ubicua* (Madrid: Dykinson, 2016), 88.
[142] M. APARICIO PÉREZ; M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 705.
[143] CONGRESO NACIONAL DEL ECUADOR 1994, [Acta No. 2 A], 34.

En el segundo debate, el texto aprobado y que consta en la Constitución de 1978 señala: "La ley protegerá el nombre, la imagen y la voz de la persona".[144] El texto sigue siendo parte del numeral que protege el derecho al honor, al buen nombre o a la intimidad. Por lo tanto, en esta Constitución, la imagen y la voz son solo medios que inadecuadamente utilizados pueden afectar a estos derechos. Aún no se los concibe como derechos independientes, manifestación de la autodeterminación informativa. Llama aún más la atención cuando la redacción establece una referencia expresa a que será la ley la que establezca las formas de protección, de tal manera que puede interpretarse que no se protege desde la dignidad humana como derecho de la personalidad, sino que se refiere a los valores económicos que se desprenden de su uso o nuevamente a las indemnizaciones que pudieran producirse por el daño civil causado al honor o a la intimidad. Contenido igual aparece en el artículo 23, numeral 8, de la Constitución Política de 1998.

Finalmente, en la Constitución de la República del Ecuador de 2008, en el Título II, Derechos, Capítulo segundo, Derechos del buen vivir, Capítulo sexto, Derechos de libertad consta el siguiente texto: "Artículo 66.- Se reconoce y garantizará a las personas: [...] 18. El derecho al honor y el buen nombre. La ley protegerá la imagen y la voz de la persona".

La misma configuración respecto de la imagen y la voz como plasmación evidente de posibles transgresiones a la honra y buen nombre se mantiene vigente en el nuevo texto constitucional. Incluso permanece inalterada la referencia a la ley acerca de la forma de protección. En cambio, dos derechos que eran parte del mismo ítem desaparecen para generar un nuevo literal o integrarse a otro: el derecho a la intimidad personal y familiar se convierte ahora en un derecho autónomo e independiente contemplado en el numeral 20 del mencionado artículo 66 de la Constitución de la República del Ecuador. Además, en esta nueva edición del artículo desaparece la mención al derecho, al nombre que ahora consta en el numeral 28 del artículo citado, como uno de los contenidos fundamentales del derecho a la identidad.

En la Mesa 1 de la Constitución de 2008 se discutió lo siguiente: "La ley protegerá el nombre, la imagen y la voz de la persona. Aquí se está dejando una brecha abierta, cuando dice que, la ley protegerá el nombre, la imagen y la voz de la persona. Cuando hablamos de la voz yo puedo, si soy malintencionada, por medio de mi voz dañar la imagen de otra. Entonces, si sería bueno que se ponga, sin dañar sin discriminar a nadie, sin dañar la honra de otras personas. Excepto en caso que tenga pruebas, que ese es otro punto".[145] Dicho de otro modo, aún sigue siendo parte de la discusión si la imagen y la propia voz solo pueden ser protegidas ante agresiones asociadas con la honra y no desde una manifestación de la autodeterminación informativa en el proceso de autoconstrucción de un individuo en sociedad.

En el mismo sentido, en el segundo debate se dice: "creo que debería hablar sobre el derecho a que se respete la reputación, la honra y, que no se utilice ni la imagen ni la voz de las personas para otros fines, o para fines que desmerezcan esta reputación o esta honra".[146]

Desde una simple lectura de la norma constitucional ecuatoriana, la imagen y la propia voz se protegen por la ley, no como derechos, sino como atributos de la personalidad; de ahí que incluso la redacción constitucional la coloca en este sentido: "La ley protegerá la imagen y la

[144] CONGRESO NACIONAL DEL ECUADOR DE 1995, [Acta No. 1], 28.
[145] ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 50], 79.
[146] Ibíd., [Acta No. 64], 105.

voz de la persona". Además, por ser parte del mismo numeral 18 en el que consta expresamente el honor y el buen nombre, la otra forma de protección sería mediante el uso indebido de la imagen y la voz para perjudicar o dañar el buen nombre de una persona.

En consecuencia, a primera vista pareciera que no ha sido aceptada en Ecuador la concepción de que la imagen y la voz sean derechos que se configuren desde la autodeterminación informativa y la conformación de la identidad de una persona en un entorno social. Su protección se encuentra regulada por la ley, como atributo de la personalidad, o en sus manifestaciones patrimoniales, ya sea por propiedad de su titular y, en todo caso, se protege la honra de las personas que pudieran verse afectadas por el uso inadecuado de imágenes y voz de una persona. Las transgresiones pueden generar responsabilidades civiles, penales o administrativas, pero también constitucionales atadas en general al derecho al honor.

Ahora bien, conforme señala el artículo 427 de la Constitución de 2008: "Las normas constitucionales se interpretarán por el tenor literal que más se ajuste a la Constitución en su integralidad. En caso de duda, se interpretarán en el sentido que más favorezca a la plena vigencia de los derechos y que mejor respete la voluntad del constituyente, y de acuerdo con los principios generales de la interpretación constitucional". En tal sentido, la Constitución ecuatoriana prevé la posibilidad de ser interpretada de forma integral, en tal sentido, se debe considerar que se afecta al honor mediante un uso inadecuado de la imagen y a la voz, pero se pude transgredir la imagen y la voz en sí misma sin necesidad de que sea otro derecho el previamente afectado. Porque la transgresión puede producirse por la captación, difusión o reproducción sin la autorización del titular siendo estas acciones posibles causas de afectaciones materiales e inmateriales del individuo.

En consecuencia, es posible reconocer la vigencia de los derechos fundamentales a la imagen y a la voz de la persona en Ecuador, en especial con las actuales condiciones de vulnerabilidad de las personas por los avances tecnológicos, ya que garantizan un espacio suficiente de protección de la persona en su interrelación con otros en sociedad, el libre desarrollo de la personalidad y el respeto a la dignidad humana que son, en suma, los objetivos de los considerados en su conjunto, derechos de la personalidad.

2.7 *Habeas data*[147] (1996)

Sobre el paulatino reconocimiento al derecho a la protección de datos personales es hito fundamental en el análisis cronológico la incorporación de la garantía del *habeas data* en la Tercera Codificación en 1996, de la Constitución de 1978.

Sixto Durán Ballén, el entonces Presidente de la República del Ecuador, mediante Consulta Popular realizada al pueblo ecuatoriano el 28 de agosto de 1994, entre varios temas, preguntó sobre la incorporación constitucional de esta nueva figura denominada *habeas data*. Aprobada la configuración constitucional por consulta mayoritaria se realizó el debate para la pertinente reforma constitucional y su respectiva codificación.

En la mencionada discusión, las primeras reacciones ante esta nueva garantía constitucional planteada por el Presidente de la República tuvieron una posición detractora que consideraba

[147] Aunque la norma ecuatoriana la escribe con tilde e inicial mayúsculas, debido a su origen en el latín, la expresión *habeas data*, no se tilda y se coloca en cursiva por ser idioma extranjero, según como lo registra la *Ortografía de la lengua española*, 2010.

que esta institución "no va a tener realización práctica, y va a constituir en definitiva un trauma inaceptable en la administración del Estado";[148] sin embargo la Comisión Constitucional del Congreso Nacional respecto de este tema consideró "que se debía robustecer los procedimientos para hacer efectivas las garantías constitucionales, y para ello adoptamos cuatro resoluciones: introducir la acción de amparo constitucional, la institución de la Defensoría del Pueblo, reformar el procedimiento de impugnación de la constitucionalidad de los actos públicos e introducir el *Habeas data*".[149]

Al final de la primera lectura del proyecto se consideró que "todo ciudadano tiene derecho, cuando menos, a conocer la información que sobre él tienen en cualquier dependencia pública".[150] Consecuentemente, la discusión dejó de centrarse en la introducción o no de esta nueva garantía en el cuerpo constitucional y dirigió sus esfuerzos a determinar su alcance. Entonces, se debatía si debía permanecer o no la excepción de acceso a documentos reservados por razones de seguridad nacional. Esta posición se sustentaba en considerar que los mayores transgresores de los datos de sus ciudadanos son los gobiernos de turno. En segundo debate la discusión se zanjó y, en consecuencia, se conservó la excepción, por la que toda persona tiene derecho de acceder a su información contenida en documentos, excepto aquellos considerados reservados por razones de seguridad nacional; dicho de otra manera, el texto se aprobó conforme la versión original enviada por el Ejecutivo.

Asimismo, en esta primera lectura del proyecto se discutió si el *habeas data*, además de información personal y de los bienes de su titular, también debía permitir el acceso a "aspectos de interés público a nivel local o nacional"[151]. Esta argumentación visibilizaba una confusión en el alcance y contenido del *habeas data* y acceso a la información pública. Esto puede deberse a que se reglaba de manera conjunta la protección de datos, como ocurre en las Constituciones de Perú y Venezuela, de tal manera que existía "una marcada tendencia a consagrar una acción especial, generalmente llamada *habeas data* impropio, frente a los supuestos en que la Administración requerida se niegue o guarde silencio frente a una concreta solicitud de información. Quiere decir que si bien el *habeas data* (en sentido estricto) se ha ido perfilando como una garantía de acceso a los datos personales, también se ha aplicado (por extensión) respecto de datos no personales, especialmente en poder de Administraciones públicas, con el objeto de hacer efectivo el derecho".[152] Actualmente, es clara la diferenciación entre *habeas data* propio, que opera sobre datos de carácter personal y *habeas data* impropio, como una vía de acceder a la información pública y que algunos autores denominaban de una manera aún más confusa como *habeas data* público.[153]

Finalmente, el texto aprobado que consta en la sección II, en el título: De las garantías de los derechos, parágrafo III, del *Habeas data*, de la Tercera Codificación en 1996, de la Constitución de 1978, expresamente señala: "Artículo 30.- Toda persona tiene derecho a acceder a los documentos, banco de datos e informes que sobre si misma o sobre sus bienes consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su finalidad. Igualmente, podrá solicitar ante el funcionario o juez competente la actualización,

[148] CONGRESO NACIONAL DEL ECUADOR 1994, [Acta No. 2 A], 61.
[149] J. TOBAR DONOSO Y J. LARREA HOLGUÍN, *Derecho constitucional ecuatoriano*, 273.
[150] CONGRESO NACIONAL DEL ECUADOR 1994, [Acta No. 2 A], 61.
[151] Ibíd.
[152] R. PUCCINELLI OSCAR, "Tipos y subtipos de hábeas data en América latina", 19.
[153] Para evitar confusiones y aclarar conceptos, incluso desde su título, el tradicional *habeas data* impropio se convirtió en la garantía de acceso a la información pública, que fuera recogida en los textos constitucionales ecuatorianos; primero como derecho en los artículos 81 de la Constitución de 1998 y 18 de la Constitución de 2008, y luego como garantía constitucional en el artículo 91 de la Constitución de 2008.

rectificación, eliminación o anulación de aquellos si fueren erróneos o afectaren ilegítimamente sus derechos. Se exceptúan los documentos reservados por razones de seguridad nacional".

Larrea Holguín en su obra *Derecho constitucional ecuatoriano*, realizada junto a Julio Tobar Donoso, y como miembro de la Junta de Notables que participó en la elaboración de la propuesta normativa, respecto del *habeas data* afirmó: "el Habeas data es una nueva garantía que consiste en la posibilidad de exigir la exhibición y rectificación de documentos o datos –incluso los contenidos en sistemas electrónicos–, para resguardar la verdad y la dignidad de las personas".[154] De esta afirmación y de la versión final del texto aprobado se pueden realizar varias precisiones:

a) El *habeas data* recoge lo que en otras legislaciones se conoce como derechos ARCO, y que en el caso del Ecuador son: el acceso, la rectificación, actualización, eliminación y anulación de los datos personales por parte de sus titulares.

b) La garantía solo operaba si es que los datos eran erróneos o existía una afectación ilegítima de los derechos de sus titulares. Se concebía como una medida de acción posterior cuando la transgresión había ocurrido, ya sea por la falta de la calidad del dato o por una consecuencia dañosa de su uso. Es decir, no era parte del contenido del *habeas data* la autodeterminación informativa que ahora se considera uno de los elementos esenciales del derecho a la protección de datos personales.

c) Es evidente la asociación de esta garantía a los medios de captación electrónica, no solo por el testimonio de uno de sus autores, antes citado, sino por la mención expresa que hace la norma constitucional respecto a *bancos de datos*.

d) Además, de la simple lectura, no existe alusión alguna a dato íntimo, esfera personal o términos similares que pudieran acercar esta garantía al derecho a la intimidad, por lo que se concluye que esta garantía no se encontraba directamente asociada a este derecho.

e) Ahora bien, en esta versión de la Constitución, el derecho a la protección de datos personales no se encontraba dentro del catálogo de derechos fundamentales. En consecuencia, tampoco podía asumirse que era garantía de un derecho autónomo e independiente reconocido plenamente, sino que, conforme la forma de estructuración del sistema de garantías de aquel entonces, esta acción constitucional era al tiempo derecho y garantía en sí misma.

Finalmente, Larrea Holguín exhortaba a que se "desarrollen prudentes disposiciones legales de procedimiento debido a la situación actual de la civilización".[155] En el mismo sentido, requería al Ejecutivo que este conjunto de reformas: amparo, *habeas data* y Defensoría del Pueblo sean puestas en vigencia, ya que la iniciativa partió del mismo Presidente de la República.[156]

Para Larrea Holguín, era al gobierno central a quien le correspondía desarrollar la institucionalidad, la reglamentación y las políticas públicas que permitieran la aplicación

[154] J. TOBAR DONOSO Y J. LARREA HOLGUÍN, *Derecho Constitucional ecuatoriano*, 274.
[155] Ibíd.
[156] Ibíd.

práctica del *habeas data*. El tema resultó ser más complejo ya que conforme el diseño constitucional, si bien el artículo 30 señalaba "toda persona tiene derecho", y por lo tanto, podría entenderse al *habeas data* como un derecho fundamental; sin embargo, por constar dentro de la sección II, denominada "De las Garantías de los Derechos", era parte del sistema de garantías constitucionales. En consecuencia, se dejó de lado el desarrollo desde la perspectiva de derecho, y más bien la difusión, aplicación y desarrollo del *habeas data* la realizó otra función del Estado: la jurisdiccional, tanto en vía ordinaria como especialmente en la vía constitucional.

En ese mismo sentido, se desarrolló la Ley de Control Constitucional, Ley No. 000. RO, No. 99 (de 2 de julio de 1997), que establecía en el capítulo De las garantías de los Derechos, artículos 37 y siguientes, a la acción de *habeas data*. La competencia para conocer de esta acción le correspondía a cualquier juez o tribunal de primera instancia del domicilio del poseedor de la información o de los datos requeridos. Asimismo, para segunda instancia, el numeral 3, del artículo 12 de la misma norma citada, señalaba entre las atribuciones y deberes del Tribunal Constitucional, el conocer y resolver las resoluciones que denieguen los recursos de *habeas corpus*, *habeas data* y amparo.

En el debate y aprobación de la Constitución Política de 1998, se vuelve a discutir sobre la garantía constitucional *habeas data*. Tanto en primer como en segundo debate, los asambleístas constituyentes hicieron varias precisiones que permiten comprender el espíritu y alcance de la garantía. A continuación, se realizará una descripción sobre los diferentes ámbitos debatidos, para tal efecto se los ha agrupado en los siguientes temas:

a) *Confusión entre habeas data y acceso a la información pública*. La versión inicial del artículo 30 del proyecto de Constitución de 1998, sometido a primer debate, señalaba que la persona tiene derecho a acceder a los documentos, banco de datos e informes sobre sí misma, pero elimina la frase *o sobre sus bienes*, y en su lugar constaba *sobre el medio ambiente*.[157]

Esta referencia equivocada al medio ambiente confundía la garantía del *habeas data*, que protege la información de la persona, con el derecho de acceso a la información pública. De ahí que varios asambleístas solicitaran su eliminación del texto.[158] El autor de la propuesta sostenía que la inclusión del medio ambiente se realiza desde la óptica de que también son titulares del *habeas data* los colectivos, y que para ellos es información fundamental la medioambiental que les afecta directamente. Todo lo cual parte de una premisa errónea, pues aunque se tratase de los colectivos como sujetos, la información relativa al medio ambiente no es personal sino pública y a ella se accede desde el derecho de las personas a ser informadas.

La confusión entre *habeas data* y acceso a la información pública también fue parte de la discusión, ya que el representante Álvarez Ulloa señalaba que el título del artículo en análisis debería llamarse "acceso a la información y habeas data pues [...] no únicamente se va a referir al acceso de información propia, o sea, sobre sí mismo, sino a algunos documentos públicos que deberían ser conocidos por las personas".[159]

[157] ASAMBLEA NACIONAL CONSTITUYENTE 1998 DE ECUADOR, [Acta No. 47], 44.
[158] Ibíd., 44-6.
[159] Ibíd., 44-5.

En otras palabras, se pretendía incluir en el contenido de la garantía constitucional del *habeas data*, el acceso a la información pública. Sin embargo, al realizar el análisis sobre la impertinencia de acceder a datos relativos al medio ambiente, como se aclaró en líneas anteriores, se esclareció también que el *habeas data* tiene como objetivo fundamental la defensa de los derechos individuales; y en consecuencia, de los datos personales de sus titulares, por lo que, en la norma citada, los representantes decidieron eliminar cualquier referencia relativa a datos ambientales o de carácter público. Finalmente, el derecho de acceso a la información pública se consagró en el artículo 81 de la Constitución de 1998.

b) *Relación directa de la garantía con el derecho a la intimidad*. Durante los debates, el representante Julio Trujillo Vásquez estableció que esta garantía "tiene relación con el peligro que la intimidad de una persona corre frente a los modernos medios de información, sobre todo, de acumulación de información sobre la persona y de difusión de esta información. Sin embargo, la realidad de nuestro país nos revela que no son solo los progresos de la ciencia y la técnica los que amenazaban nuestra intimidad, sino muchos otros mecanismos que de suyo debieron ser atendidos por otras instituciones".[160] Por su parte, otro represente, Orlando Alcívar Santos, sostuvo una posición similar, pues señalaba que "lamentablemente los avances tecnológicos han hecho que el hombre no tenga la intimidad total que tenía antes, el *habeas data* es eso, es una protección a la intimidad, ante la agresión tecnológica".[161]

Se han citado expresamente estas referencias al debate de aprobación del texto constitucional, puesto que en su versión antecesora, ya hemos concluido que no había dicha asociación y que el *habeas data* aparecía como materialización directa de los derechos ARCO. En cambio, en la nueva propuesta constitucional, por manifestación expresa de sus autores constituyentes, el *habeas data* estaba dirigido a proteger el derecho a la intimidad, a través de los derechos ARCO. Anotándose nuevamente que no se encontraba dentro del catálogo de derechos fundamentales el derecho a la protección de datos personales.

c) *Referencia a la confidencialidad y a la reserva de fuentes periodísticas*. En los debates se discutió la importancia de guardar el secreto profesional y se aclaró que "el *habeas data* no podrá afectar el secreto de la fuente de la información periodística".[162] En consecuencia, se decidió la incorporación de este derecho en la parte pertinente relativa al derecho a la comunicación (artículo 81, inciso segundo, de la Constitución de 1998).

d) *Autoridades competentes para conocer del habeas data*. El artículo 30 del proyecto de Constitución señalaba que en caso de oposición, el "interesado de por sí o por medio de su representante, podrá acudir a cualquier juez o tribunal de primera instancia, para que ordene el acceso, actualización, rectificación, eliminación o anulación, según sea el caso". Se consideró innecesaria la referencia explícita a la legitimación activa y a la autoridad competente, porque la Ley de Control Constitucional la establecía y porque la Constitución no debe ser reglamentaria.[163] Asimismo, en esta reforma constitucional se discutió si el Defensor del Pueblo debía

[160] Ibíd., 47.
[161] Ibíd., 48.
[162] Ibíd., 44.
[163] Ibíd., 41.

tener entre una de sus competencias la de patrocinar acciones de *habeas data*;[164] no obstante, dicha incorporación no fue aceptada.

e) *Indemnización por daños y perjuicios causados*. En el artículo 30 de la Tercera Codificación de 1996, de la Constitución de 1978, relativa al *habeas data*, no constaba referencia alguna respecto a la posibilidad de solicitar indemnización por daños y perjuicios. Para el debate constitucional de 1998 se planteó el siguiente texto para su análisis: "Artículo 30.- [...] Igualmente podrá solicitar ante el funcionario, la actualización, rectificación, eliminación, o anulación de aquellas, si fueren erróneos o afectaren ilegítimamente sus derechos. Se exceptúa los documentos reservados por razones de seguridad nacional. En caso de oposición el interesado de por sí o por medio de representante, podrá acudir a cualquier juez o tribunal de primer instancia para que ordene el acceso, actualización, rectificación, eliminación, o anulación, según sea el caso. El perjudicado podrá demandar del responsable del archivo o banco de datos, la reparación de los perjuicios que se le hubieren causado por la información errónea o de sus bienes".[165]

La Comisión Constitucional para segundo debate elaboró un texto que simplificaba la redacción y que aclaraba que era suficiente para solicitar la indemnización, la falta de atención que cause perjuicio, por parte del funcionario, respecto de la solicitud acceso, actualización, rectificación, eliminación, o anulación. En este sentido la norma consta descrita de la siguiente forma: "Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización".[166] Dicho de otra manera, no se necesita demostrar que era errónea la información personal o de sus bienes, como señalaba la primera versión del texto, sino únicamente que la falta de atención del funcionario que se negó a corregir los datos le ha causado algún tipo de daño.

f) *El derecho a solicitar la rectificación provienen de que los datos sean falsos o inexactos*. Es relevante mencionar un pronunciamiento realizado en segundo debate por el representante Julio César Trujillo: "el derecho a solicitar la rectificación no proviene del derecho al *habeas data*, sino del hecho de que los datos que constan en los bancos sean falsos o inexactos".[167]

Dicha afirmación no se contextualizó sobre bases de datos que por ley deban recopilarse y en la que podría tener cierto asidero, puesto que la obligatoriedad de mantener los datos sería obvia, y por lo tanto, únicamente facultaría a su titular a solicitar su rectificación si los datos fueren errados. Por el contrario, esta aseveración se ha realizado desde una perspectiva amplia, por la que los responsables de los ficheros públicos o privados podían recopilar los datos de las personas en sus bases siempre que no fueren equivocados. Está aún lejana la aproximación del *habeas data* como garantía del derecho a la protección de datos personales, su contenido se asimilaba a la protección a la intimidad y a la veracidad de los datos, pero no a su titularidad y a las consecuencias de la utilización de estos; es decir, se concluye que no existe el derecho a la autodeterminación informativa en el contenido del *habeas data* de la Constitución de 1998.

[164] Ibíd., 36.
[165] Ibíd., 43.
[166] ASAMBLEA NACIONAL CONSTITUYENTE DE 1998 DE ECUADOR, [Acta No. 80], 20.
[167] Ibíd., [Acta No. 81], 8.

g) *La seguridad nacional como excepción al habeas data*. Al respecto, se discutió, tal como en la anterior Constitución, que todos los datos de las personas deben ser accesibles a sus titulares incluso aquellos que son recabados con motivo de seguridad nacional, porque "precisamente la seguridad nacional es donde más se pueden recoger datos falsos".[168] Sin embargo, la Comisión Constitucional presentó dos posturas al respecto, la primera que pretendía una eliminación completa del inciso y la segunda, que fue la finalmente aprobada, que salvaguarda la posibilidad de acceso a dicha información siguiendo un procedimiento previamente establecido en la ley. Así, el texto final es el siguiente: "La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional". Es decir, la nueva norma constitucional no establece una excepción general de acceder a documentos reservados como lo hacía su predecesora, sino que determina un mecanismo legal que permita el acceso justificado a esta información.

La versión final del artículo 94 de la Constitución de 1998 textualmente dice:

> Artículo 94.- Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional.

De lo analizado, tanto en las reformas a la Constitución de 1978, codificada en 1996 y de su inmediata sustitutiva, la Constitución de 1998, se colige que es mediante el *habeas data* que se introduce en el ordenamiento jurídico ecuatoriano una aproximación real al contenido esencial del derecho a la protección de datos personales, dado que, por primera vez, aparece un nuevo ámbito de protección respecto de los datos personales con especial énfasis en los medios electrónicos.

En la versión de la reforma de 1996, la garantía del *habeas data* no estaba asociada directamente a un derecho fundamental específico, sino que, tal como se concebía en aquella época, la garantía se consideraba acción y derecho al mismo tiempo. De esta manera el *habeas data* se concebía como un derecho de acceso, rectificación, actualización, eliminación o anulación de datos personales en poder de terceros.

Posteriormente, con la Constitución de 1998, nuevamente aparece el *habeas data*, pero esta vez se lo asocia directamente como garantía del derecho a la intimidad, por referencias de los constituyentes que lo elaboraron, aunque de su texto no se desprende alusión alguna a una protección relativa al entorno familiar, personal o íntimo. En conclusión, parece que aunque no existía en Ecuador derecho a la protección de datos personales, la garantía de *habeas data* era suficiente para efectivizar parte de su contenido esencial relativo a los derechos ARCO; sin embargo, no se tutelaba la autodeterminación informativa y tampoco se recogían los principios característicos que lo definen y completan.

3. Contextualización constitucional del Ecuador en el período 2008-2019

[168] Ibíd., [Acta No. 47], 47.

Han transcurrido 187 años desde la conformación del Estado ecuatoriano en 1830. Durante este tiempo, las distintas realidades políticas, económicas y sociales han provocado un cambio normativo constitucional profundo y complejo. Ecuador ha atravesado tres etapas constitucionales: la primera etapa, de formación del Estado; la segunda, de consolidación; y la tercera de reciente nacimiento denominada *Garantismo*.

Se propone contextualizar la situación constitucional del Ecuador en el período 2008-2019. Este período comprende desde la promulgación de la Constitución de la República del Ecuador en el 2008 hasta la fecha.

Para el año 2006 es electo Rafael Correa como Presidente del Ecuador; entre sus propuestas de campaña propuso una consulta popular para elegir a una Asamblea Constituyente que prepare un nuevo texto constitucional. La consulta se realizó en abril de 2007. Para el 28 de septiembre de 2008 la Constituyente terminó su labor y aprobó la nueva Constitución de Ecuador que entró en vigencia el 20 de octubre del mismo año. "Es una Constitución que recoge, en buena parte, instituciones y derechos de la Constitución codificada de 1998, pero al tiempo presenta un desarrollo más detallado y una serie de innovaciones importantes...".[169]

En el escenario latinoamericano se conjugan situaciones similares a nivel político, social y económico, en especial en México, Argentina, Colombia y Brasil, donde las reivindicaciones sociales y las marcadas crisis políticas y económicas permitieron el nacimiento de lo que varios autores denominan como *constitucionalismo latinoamericano*.[170] Los casos de Venezuela, Bolivia, Ecuador y desde la jurisprudencia en Colombia son parte de este proceso, que por la impronta de los países andinos se nombra constitucionalismo *desde el Sur*.[171]

En Ecuador, el artículo 1 de la Constitución del 2008 define al Estado ecuatoriano como un Estado de derechos y justicia,[172] social, democrático, soberano, independiente, unitario,

---

[169] A. GRIJALVA JIMÉNEZ, *Constitucionalismo en Ecuador* (Quito: Corte Constitucional para el Período de Transición, 2012), 25.

[170] R. ÁVILA SANTAMARÍA, A. ACOSTA Y E. MARTÍNEZ, *El neoconstitucionalismo transformador: el Estado y el derecho en la Constitución de 2008* (Quito: Abya-Yala / Universidad Andina Simón Bolívar, 2011), 17. Ahora bien, cabe indicar que "Desde mediados de los años ochenta, a partir de la Constitución de Brasil de 1988, y en especial en los años noventa, en América Latina se inició un intenso periodo de cambios constitucionales en casi todos los países; se adoptan nuevas constituciones o se introducen reformas muy importantes.
Es obvio que existen diferencias muy importantes entre los cambios constitucionales en los distintos países. Sin embargo, a pesar de estas diferencias nacionales, esta oleada de reformas y nuevas constituciones en América Latina tiene algunos rasgos comunes, que podemos reagrupar en aquellos más relativos a la llamada 'parte dogmática' de la Constitución y otros más vinculados a la llamada 'parte orgánica', por recordar esa vieja, discutible, pero pedagógica distinción de algunos enfoques tradicionales del derecho constitucional. Según eta distinción, la parte dogmática de una Constitución hace referencia a aquellos apartados del texto constitucional que definen los principios ideológicos que orientan al Estado y que establecen los derechos y deberes de las personas. Por su lado, la parte orgánica es aquella que precisa cuáles son los principales órganos del estado y cuáles son sus atribuciones. Finalmente, un poco entre los dos, se encuentran los mecanismos de participación ciudadana y la regulación constitucional de los partidos, que son al mismo tiempo una expresión de los derechos políticos (y por ello algunos autores la vinculan a la parte dogmática) y una forma de integración de los órganos políticos (por lo que otros autores suelen tratar estos aspectos al estudiar la parte orgánica)". Véase R. UPRIMNY YEPES, "Reflexiones tentativas sobre Constitución, economía y justicia constitucional en América Latina", citado en *Genealogía de la justicia constitucional ecuatoriana* (Quito: Corte Constitucional para el Período de Transición, 2011), 58.

[171] Véase G. PISARELLO, *Un largo termidor*, 189.

[172] Ninguna otra Constitución en el mundo señala las características de "derecho**s** y justicia"; para algunos autores estas precisiones no son más que pronunciamientos retóricos; en cambio para los ideólogos detrás del cambio constitucional reflejan una nueva concepción de entender al Estado, a los derechos y a las garantías de los ciudadanos.

intercultural, plurinacional y laico. Acoge la propuesta de Ferrajoli sobre *democracia sustancial*,[173] garantista de derechos fundamentales, no solo de aquellos de contenido patrimonial, y la adapta a las particularidades propias de la región[174] marcada por la diversidad cultural y la coexistencia de diversos pueblos indígenas, la plurinacionalidad, el diálogo intercultural y la Naturaleza o *Pacha Mama* como sujeto con titularidad y derechos propios reconocidos en la Carta Magna.

Acerca del contenido de los derechos y sus garantías, la Constitución ecuatoriana de 2008 clasifica a los derechos desde su contenido temático: derechos del buen vivir, derechos de las personas y grupos de atención prioritaria, derechos de las comunidades, pueblos y nacionalidades, derechos de participación, derechos de libertad, derechos de la naturaleza, derechos de protección.

Los elementos caracterizantes del constitucionalismo ecuatoriano, y que coincide con lo que varios autores –entre los que destacan Fariñas Dulce[175], Rodríguez[176] y Ronconi[177]- y afirman constituye el constitucionalismo latinoamericano y andino, acerca de derechos y garantías, podrían simplificarse en: mayor y mejor reconocimiento de los derechos, estableciendo un igual estatuto jurídico para los derechos individuales y los colectivos de tal forma que cualquier derecho puede exigirse eventualmente de forma colectiva;[178] eliminación de la clasificación de derechos de primera, segunda y tercera generación, pues se establece la complementariedad, justiciabilidad y la jerarquía igual de todos los derechos; [179] ampliación del contenido de los derechos constitucionales; reconocimiento de los demás derechos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades necesarios para su desenvolvimiento;[180] y generación de un sistema de garantías integrales, es decir, garantías jurisdiccionales vinculantes, adecuadas y eficaces para la protección de todos los derechos constitucionales por parte de todas las funciones del estado e incluso de los sujetos privados que están obligados a efectivizar los derechos constitucionales. Nacen otros tipos de garantías, anteriormente no reconocidas, como las garantías normativas,[181] políticas y

[173] Véase L. FERRAJOLI, *Derechos y garantías: la ley del más débil*, 4a. ed. (Madrid: Editorial Trotta, 2004), 23.
[174] R. ÁVILA SANTAMARÍA Y OTROS, *El neoconstitucionalismo transformador*, 17.
[175] M. FARIÑAS DULCE. *Democracia y pluralismo. Una mirada hacia la emancipación*, (España: Dikynson, 2013), 97.
[176] F. RODRÍGUEZ, *Hacia un Ius Constitucionale Commune en materia de reconocimiento y protección de minorías: La jurisdicción indígena en Colombia, Ecuador y Bolivia,* (Colombia: U. Externado de Colombia, 2017), 12-14.
[177] L. RONCONI, Derecho a la educación e igualdad como no sostenimiento, (Colombia: U. Externado de Colombia, 2018), 21.
[178] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR [2008], "Artículo 11: El ejercicio de los derechos se regirá por los siguientes principios: 1. Los derechos se podrán ejercer, promover y exigir de forma individual o colectiva ante las autoridades competentes; estas autoridades garantizarán su cumplimiento".
[179] Ibíd., "Artículo 11: El ejercicio de los derechos se regirá por los siguientes principios: [...] 6. Todos los principios y los derechos son inalienables, irrenunciables, indivisibles, interdependientes y de igual jerarquía".
[180] Ibíd., "Artículo 11: El ejercicio de los derechos se regirá por los siguientes principios: [...] 7. El reconocimiento de los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos, no excluirá los demás derechos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades, que sean necesarios para su pleno desenvolvimiento".
[181] Ibíd., "Artículo 84: La Asamblea Nacional y todo órgano con potestad normativa tendrá la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales, y los que sean necesarios para garantizar la dignidad del ser humano o de las comunidades, pueblos y nacionalidades. En ningún caso, la reforma de la Constitución, las leyes, otras normas jurídicas ni los actos del poder público atentarán contra los derechos que reconoce la Constitución".

servicios públicos y participación ciudadana.[182] Además, la obligatoriedad de dictar reparación integral y no la simple indemnizatoria en caso de vulneración de derechos.[183]

Conforme señala la propia Corte Constitucional en su jurisprudencia, elemento fundamental es el reconocimiento de la Constitución como norma vinculante, con valores, principios y reglas propias que guían la actuación de los poderes públicos. En este sentido, juega un factor preponderante la actividad de un juez garante de la democracia constitucional y de la protección y reparación de los derechos constitucionales de las personas. Se parte desde la premisa de la constitucionalización de la justicia ecuatoriana, en la cual juezas y jueces de la República regulan por medio de sus fallos las realidades sociales mediante jurisprudencia vinculante.[184]

Otro de los contenidos distintivos de la Constitución ecuatoriana, que la identifica con lo que denominan algunos autores como el constitucionalismo andino, es la incorporación del *sumak kawsay* o buen vivir.[185] Desde esta perspectiva, los derechos constitucionales se agrupan en aquellos que integran y viabilizan el progreso de los ciudadanos, no solo desde la visión tradicional de desarrollo económico, sino desde la integralidad del ser humano con el objetivo de mejorar la calidad de vida, el respeto a la naturaleza, la generación de capacidades, la reducción de las brechas sociales y territoriales, el desarrollo de nuevos valores y conceptos ciudadanos, comunitarios y colectivos; y una revolución educativa.[186] En este sentido, a nivel normativo intenta afianzar derechos como: al agua y alimentación, ambiente sano,

[182] Ibíd., "Artículo 85: La formulación, ejecución, evaluación y control de las políticas públicas y servicios públicos que garanticen los derechos reconocidos por la Constitución, se regularán de acuerdo con las siguientes disposiciones: | 1. Las políticas públicas y la prestación de bienes y servicios públicos se orientarán a hacer efectivos el buen vivir y todos los derechos, y se formularán a partir del principio de solidaridad. | 2. Sin perjuicio de la prevalencia del interés general sobre el interés particular, cuando los efectos de la ejecución de las políticas públicas o prestación de bienes o servicios públicos vulneren o amenacen con vulnerar derechos constitucionales, la política o prestación deberá reformularse o se adoptarán medidas alternativas que concilien los derechos en conflicto. | 3. El Estado garantizará la distribución equitativa y solidaria del presupuesto para la ejecución de las políticas públicas y la prestación de bienes y servicios públicos. | En la formulación, ejecución, evaluación y control de las políticas públicas y servicios públicos se garantizará la participación de las personas, comunidades, pueblos y nacionalidades".

[183] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR [2008], "Artículo 86: Las garantías jurisdiccionales se regirán, en general, por las siguientes disposiciones: [...] 3. La jueza o juez resolverá la causa mediante sentencia, y en caso de constatarse la vulneración de derechos, deberá declararla, ordenar la reparación integral, material e inmaterial, y especificar e individualizar las obligaciones, positivas y negativas, a cargo del destinatario de la decisión judicial, y las circunstancias en que deban cumplirse. Las sentencias de primera instancia podrán ser apeladas ante la corte provincial. Los procesos judiciales sólo finalizarán con la ejecución integral de la sentencia o resolución".

[184] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0023-2008-HD], ROS No. 518, (30 de Enero de 2009), 8.

[185] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR [2008], "Artículo 277: Para la consecución del buen vivir, serán deberes generales del Estado: | 1. Garantizar los derechos de las personas, las colectividades y la naturaleza. | 2. Dirigir, planificar y regular el proceso de desarrollo. | 3. Generar y ejecutar las políticas públicas, y controlar y sancionar su incumplimiento. | 4. Producir bienes, crear y mantener infraestructura y proveer servicios públicos. | 5. Impulsar el desarrollo de las actividades económicas mediante un orden jurídico e instituciones políticas que las promuevan, fomenten y defiendan mediante el cumplimiento de la Constitución y la ley. 6. Promover e impulsar la ciencia, la tecnología, las artes, los saberes ancestrales y en general las actividades de la iniciativa creativa comunitaria, asociativa, cooperativa y privada".
"Artículo 387.- Será responsabilidad del Estado: [...] 2. Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, al sumak kawsay".

[186] Secretaría Nacional de Planificación y Desarrollo [Senplades], 2013, 16.

comunicación e información, cultura y ciencia, educación, hábitat y vivienda, salud, trabajo y seguridad social, entre otros.

Como vemos, la Constitución ecuatoriana está marcada por una fuerte ideología, que se categoriza a sí misma como *socialista del siglo XXI o socialismo del Buen Vivir*, y que se sustenta como aquella que "articula la lucha por la justicia social, la igualdad y la abolición de los privilegios, con la construcción de una sociedad que respete la diversidad y la naturaleza".[187]

La Constitución de 2008 recoge instituciones progresistas del derecho europeo, por lo que, varios autores afirman que en el Ecuador se ha desarrollado un sistema constitucional al que denominan neoconstitucionalismo.[188] Otros autores, detractores de estas teorías, consideran que solo se ha renombrado una visión constitucional antiquísima: el iusnaturalismo.[189]

En cambio, otros como Ramiro Ávila Santamaría consideran que no solo se trata de un nuevo constitucionalismo sino que por, su contenido original, con distintivos andinos, se perfila como el *neoconstitucionalismo andino o transformador*.[190] Sin embargo, el contenido de la Constitución no necesariamente coincide con la realidad ecuatoriana.[191] Si bien la Constitución contiene preceptos valiosos; sin embargo estos no han podido ser ejecutados, incluso por el propio gobierno que los impulsó. Esta realidad no justifica su inaplicabilidad sino que es *deber ser* de la sociedad y del Estado su efectiva vigencia.[192]

De otro lado, otros autores ecuatorianos señalan que si bien la Constitución ha desarrollado el catálogo de derechos, no ha logrado que su parte orgánica garantice el cumplimiento y respeto de los derechos y la vigencia de una democracia deliberativa y participativa, pese a las varias instituciones creadas para el efecto. Por lo tanto, es una Constitución que en su estructura carece de los elementos normativos coherentes para materializar su propuesta.

Asimismo, existen otras novedades en el texto constitucional ecuatoriano, en la descripción y estructura del Estado, en la creación de los cinco poderes,[193] en el marcado intervencionismo

---

[187] Ibíd., 32.

[188] Sobre el Neoconstitucionalismo, véase G. ZAGREBELSKY, *El derecho dúctil*, 9a. ed. (Madrid: Editorial Trotta, 2009); también L. FERRAJOLI, *Derechos y garantías: la ley del más débil*, citado en L. PRIETO SANCHIS, *Justicia constitucional y derechos fundamentales*, Trotta, Madrid, 2009.

[189] Véase L. PRIETO SANCHÍS, J. A. GARCÍA AMADO Y C. BERNAL PULIDO.

[190] "En el segundo momento se describe las respuestas dadas por el derecho a la crisis, mediante lo que se ha venido conociendo como «neoconstitucionalismo», que tiene algunos matices diferenciados entre el neoconstitucionalismo europeo occidental, de corte positivista contemporáneo, y que se basa en el modelo alemán, italiano y español; el neoconstitucionalismo latinoamericano, que comienza con la constitución brasileña y le sigue la colombiana, que se caracterizan por reconocer nuevos derechos y de forma decidida los derechos sociales; y el constitucionalismo andino, en particular a partir de las Constituciones boliviana y ecuatoriana, que introducen, entre otros aspectos novedosos, la noción de pluriculturalidad, interculturalidad, la *pachamama* y el *sumak kawsay* a los avances europeos y latinoamericanos". Véase R. ÁVILA SANTAMARÍA, 2011, 18.

[191] J. ECHEVERRÍA, "El Estado en la Nueva Constitución", en *La Nueva Constitución del Ecuador. Estado, derechos e instituciones* (Quito: Corporación Editora Nacional, 2009), 20.

[192] R. ÁVILA SANTAMARÍA Y OTROS, *El neoconstitucionalismo transformador*, 19.

[193] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR [2008], "Artículo 225: El sector público comprende: | 1. Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral y de Transparencia y Control Social". Véanse también los artículos 118 a 140, Función Legislativa; artículos 141 a 166, Función Ejecutiva; artículos 167 a 203, Función Judicial y Justicia Indígena; artículos 204 a 216, Función de Transparencia y Control Social; y los artículos 217 a 224, Función Electoral.

estatal en la economía,[194] el *hiperpresidencialismo*, entre otros. Luis Fernando Torres sostiene que "el modelo económico y político del gobierno encauzó la fuerza del poder constituyente, a tal punto que el proceso constituyente se puso al servicio de un socialismo altamente racionalista y utilitario cuya lógica no fue otra que la de multiplicar los beneficios que podía distribuir el grupo gobernante en su condición de administrador del Estado. Con esta visión, desde el ejecutivo, se magnificó el rol del Estado, sin importar lo que ocurriera con el mercado y las libertades individuales".[195]

Sin duda, estas disquisiciones intelectuales son difíciles, profundas e ideológicas. "Como la del propio constitucionalismo, es una historia hecha de múltiples historias; una historia plural, conflictiva y abierta, en la que, más allá de ciertas líneas de continuidad, siempre es posible detectar avances y retrocesos; en el contenido de los derechos, en la definición de sus titulares y de los sujetos obligados y en los mecanismos de tutela o garantía".[196]

Esta contextualización constitucional del Ecuador permite comprender la realidad ecuatoriana, reglas, valores y principios que gobiernan su ordenamiento jurídico y que permiten delimitar el contenido, naturaleza, alcance, dimensiones de sus derechos y garantías constitucionales vigentes. En suma, desarrolla el marco normativo aplicable al derecho a la protección de datos personales, a la garantía jurisdiccional del *habeas data* y a otras garantías constitucionales relacionadas que, pese a su vigencia, el Estado ecuatoriano está en deuda en su implementación.

4. Protección de datos personales en la Constitución de la República del Ecuador de 2008

En los títulos precedentes se ha realizado un análisis histórico normativo que establece el desarrollo cronológico hasta el contenido vigente en la Constitución de 2008,[197] en adelante CRE, de cada uno de los derechos constitucionales relacionados con la protección de datos personales como son: la inviolabilidad del domicilio, la inviolabilidad de la correspondencia, el honor, la intimidad y la propia imagen y voz. Asimismo, el antecedente inmediato y directo del *habeas data* como garantía constitucional.

Esta delimitación, sobre la base de la evolución y de la exclusión de las características propias de otros derechos constitucionales, permite trazar elementos que definan el contenido, naturaleza, alcance y dimensiones del derecho a la protección de datos personales y de la garantía jurisdiccional del *habeas data*.

---

[194] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR [2008], "Artículo 275: El régimen de desarrollo es el conjunto organizado, sostenible y dinámico de los sistemas económicos, políticos, socio-culturales y ambientales, que garantizan la realización del buen vivir, del *sumak kawsay*. |El Estado planificará el desarrollo del país para garantizar el ejercicio de los derechos, la consecución de los objetivos del régimen de desarrollo y los principios consagrados en la Constitución. La planificación propiciará la equidad social y territorial, promoverá la concertación, y será participativa, descentralizada, desconcentrada y transparente. | El buen vivir requerirá que las personas, comunidades, pueblos y nacionalidades gocen efectivamente de sus derechos, y ejerzan responsabilidades en el marco de la interculturalidad, del respeto a sus diversidades, y de la convivencia armónica con la naturaleza".

[195] L. F. TORRES, "El presidencialismo constituyente y el Estado constitucional de Montecristi", en *La Nueva Constitución del Ecuador. Estado, derechos e instituciones* (Quito: Corporación Editora Nacional, 2009), 431.

[196] M. CARRASCO DURÁN Y J. PÉREZ ROYO, *Curso de derecho constitucional*, 576.

[197] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR [2008].

Dentro de este proceso de delimitación es indispensable la comprensión de las reglas, valores y principios del actual ordenamiento jurídico ecuatoriano, pues en esta perspectiva se puede configurar una adecuada aplicación directa e interpretación; y un propicio desarrollo normativo y de políticas públicas, que serán materia de análisis en el capítulo final de este trabajo doctoral.

La Constitución ecuatoriana de 2008 reconoce, por primera vez, el derecho a la protección de datos personales. En la nueva organización constitucional, el Título II, en nueve capítulos, amplía y fortalece el sistema de derechos de las personas, las comunidades, pueblos, nacionalidades, colectivos e incluso los de la naturaleza. De tal forma que se eliminan las generaciones y la jerarquización de los derechos. La protección de datos personales consta en el capítulo sexto relativo a los derechos de libertad de las personas. Aquellos derechos que permiten el ejercicio de las libertades individuales en sus distintos aspectos, si bien propios de personas físicas e individuales, inherentes y básicas, pues tienen como antecedente inmediato a la dignidad del ser humano, también pueden ser extendidos a las personas jurídicas, en virtud del principio de universalización[198] que consta en el artículo 10 de la Carta Magna, si son de aquellos que les correspondan, según su naturaleza social y siempre en atención a la definición constitucional de los derechos de los que se trate.[199]

Asimismo, la Constitución distingue el derecho al honor y al buen nombre, de la protección legal de la imagen y la voz de la persona, del derecho a la intimidad personal y familiar, ya que los consagra en distintos numerales, esto es el 18 y el 20, respectivamente, del citado artículo 66 de la Constitución.

En el mismo sentido, la nueva Constitución de 2008 consagra la garantía constitucional del *habeas data* con un contenido más amplio, que ya no solo se asocia a documentos o datos personales contenidos en soporte electrónico, sino también aquellos constantes en soporte material, por ejemplo.

Adicionalmente, la nueva concepción de las garantías concertada en el texto constitucional establece una protección ampliada de todos los derechos fundamentales, de los cuales por su naturaleza se asocia al *habeas data* no solo al derecho a la intimidad, sino al buen nombre, el honor, la propia imagen y la voz; así como, al autónomo e independiente y recién incluido en el catálogo de derechos fundamentales, derecho a la protección de datos personales. Sobre este tema, se analizará más a profundidad en el subtítulo que se refiere a esta garantía constitucional.

4.1 Debates constitucionales sobre el derecho a la protección de datos personales

Tradicionalmente, para conocer el espíritu de las leyes o de las normas, se acude a las discusiones o debates realizados por los representantes del pueblo, en este caso los asambleístas constituyentes. En general, el debate constitucional que se realiza mediante argumentos, contrargumentos, acuerdos y posiciones permite delinear aquellos elementos que determinan el contenido, enfoque o precisión de un texto constitucional.

Lamentablemente, el proceso de aprobación de los textos de la Constitución de 2008 no permite conocer a detalle las discusiones sobre cada uno de los artículos o numerales que lo

[198] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0023-2008-HD], 8.
[199] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR PARA EL PERÍODO DE TRANSICIÓN, [Sentencia No. 068-2010-SEP-CC], 13.

conforman; en este caso no se puede conocer a profundidad el análisis de cada uno de los derechos. Cada mesa realizaba un informe que contiene un grupo de artículos asignados. En este caso, la Mesa 1 tenía a su cargo los artículos relacionados con los derechos fundamentales. Tanto en la sesión de primer y segundo debate se leyeron y discutieron los artículos en bloque. Los asambleístas intervinieron por un lapso de 20 minutos sobre la totalidad de los artículos.

Las observaciones específicas se enviaban por escrito. El mayor tema de discusión fue sobre el derecho a la vida desde la concepción, por las implicaciones políticas, sociales y religiosas del tema; por lo que, la mayoría de las intervenciones hacen referencia a este problemática y a sus repercusiones jurídicas. No obstante, otro de los temas que fue debatido, por su novedad y difícil comprensión, aunque con menor énfasis, fue el derecho a la protección de datos personales. De modo que, a continuación se recogen algunas observaciones que fueron tomadas en cuenta para la modificación de su texto hasta su versión final.

Las opiniones y debates sobre este derecho dependían de la comprensión de su naturaleza. Un grupo de asambleístas seguían mirando al derecho a la protección de datos personales como exclusiva manifestación de la intimidad, mientras que otro bloque ya lograba divisar su individualidad y autonomía sobre todo desde la perspectiva de los avances tecnológicos y la automatización de los datos personales.

Si bien, se reconoce que la Constitución de 1998 fue progresista y generosa en el reconocimiento de derechos,[200] la nueva Carta Magna de 2008 presenta un nuevo articulado relativo a los derechos fundamentales en el que se realizaron varias modificaciones y se introdujeron nuevos derechos, entre ellos la protección de datos personales. A diferencia de casi todos los otros derechos que eran tratados, discutidos y aprobados por unanimidad, la Mesa No. 1 de la Asamblea Constituyente, en voto de mayoría que contó con un voto en contra y una abstención, presentó un nuevo derecho a incluirse en el texto constitucional, cuya versión inicial decía lo siguiente: "Derecho a la protección de datos de carácter personal: a) El Estado garantiza el derecho a decidir sobre los datos personales; b) La ley regulará la recolección, archivo, procesamiento, distribución o difusión de la información de esos datos. Para todo esto se requerirá la autorización del titular o la prescripción de la ley".[201]

En el primer debate los asambleístas evidenciaron la realidad social y tecnológica que hace necesaria su incorporación en el inventario de derechos de las personas. Por ejemplo, el asambleísta Lenin Hurtado en una de las intervenciones mencionó lo siguiente:

> Aquí se señaló que era peligroso hablar de eso, no creo que es peligroso, es oportuno y es oportuno porque los datos de carácter personal, nunca como hoy han estado más amenazados, no me refiero a los escándalos alrededor de la Asamblea Constituyente, sino que el mismo desarrollo de la tecnología de la información y la comunicación plantean nuevos peligros a los datos de carácter personal, por eso me parece que cuando el texto propuesto habla de protección contra el tratamiento o el procesamiento, me parece que hay que agregar procesamiento, tratamiento automatizado, porque hay el peligro en los datos de carácter personal, que procesado automáticamente, pueden derivar en información que sea en contra de la misma persona titular de esos datos.[202]

[200] ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 50], 31.
[201] Ibíd., 35-6.
[202] Ibíd., 133-4.

Es decir, la discusión se centra en las afectaciones que las nuevas tecnologías pueden llegar a producir respecto de las personas y sus datos en el desarrollo cotidiano del ejercicio de sus libertades individuales.

En un segundo momento, la Asamblea Constituyente dejó de discutir la importancia y relevancia actual de este derecho y las cuestiones se concentraron en determinar la naturaleza jurídica del derecho. A tal punto que, incluso el asambleísta Luis Hernández llegó a proponer un texto que en lugar de consagrar derechos individuales de cada uno de los derechos de la personalidad estudiados (protección de datos personales, intimidad, honor, inviolabilidad de correspondencia y de domicilio) se los reunían en una sola propuesta que mantenía un enfoque de intimidad negativa. Dicho de otro modo, se pretendía proteger a las personas únicamente de las agresiones, ofensas o daños a la intimidad en sus manifestaciones: domicilio, correspondencia o datos íntimos.[203] Además, se intentó, sin resultado, incrementar un elemento adicional en el texto constitucional: el tratamiento automatizado.[204]

Entonces, se precisó que el derecho a la protección de datos personales era más que una manifestación informática del derecho a la intimidad personal y familiar, pues se vinculó con los avances tecnológicos y la automatización de la información que puede generar conclusiones equívocas que perjudiquen al titular del dato personal.[205] Finalmente, en segundo debate el asambleísta Romel Rivera aclaró que "el derecho a la protección de carácter personal, constituye el control que a cada una de las personas le corresponde sobre la información que les concierne personalmente sea íntima o no".[206] Así, la autodeterminación informativa resulta constituir elemento sustancial del contenido del derecho.

Esta conclusión no fue fácil de alcanzar, pues el asambleísta César Rohón, en postura contraria, argumentó: "nadie puede decidir sobre sus datos personales, tú naces con ellos, y el Estado no puede inmiscuirse en ello, ni tú mismo puedes cambiar tus datos personales [...] Que toda persona tiene derecho. Creo que tiene que reescribirse de otra manera, porque decidir sobre los datos personales, conlleva a la intención de que puedo cambiar mis nombres. Entonces mañana alguna persona que tiene problemas con la justicia o un juicio de deuda, puede cambiarse de nombre".[207] La aseveración demuestra una confusión entre el reconocimiento a la autodeterminación informativa como parte del contenido esencial del derecho a la protección de datos de carácter personal y la necesidad de establecer límites, como ocurre con otros derechos, al derecho a la protección de datos.

Del análisis de la versión original de la norma en la que constaban únicamente dos literales se puede concluir que la verdadera discusión no se refería a la autodeterminación informativa, sino que se centraba en establecer límites al derecho. El literal a) no contemplaba ningún límite, solo mencionaba la obligación del Estado de garantizar a las personas el derecho a decidir sobre sus datos de carácter personal. Mientras que el literal b) mencionaba expresamente que la ley regulará la recolección, archivo, procesamiento, distribución o difusión de la información de esos datos. Al estar en literales distintos, se argumentó que

[203] "Propongo que por ejemplo, se hable de un derecho a la intimidad personal y de la familia y propongo el siguiente articulado. Toda persona tiene derecho a la inviolabilidad de su vida familiar y privada, de su domicilio, de su correspondencia, así como de sus relaciones postales y de sus telecomunicaciones, toda persona tiene derecho a ser protegido contra el empleo ofensivo de sus datos personales" Ibíd., 105.
[204] Ibíd., 134.
[205] Ibíd.
[206] ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 64], 42.
[207] Ibíd., 58.

podría interpretarse erróneamente, que la limitación legal solo se refería los derechos ARCO contenidos en este segundo literal y no a la autodeterminación informativa. En este sentido, se arguyó:

> [...] que las personas tendremos un derecho absoluto a decidir sobre nuestros datos personales, se está creando una definición demasiado amplia, un derecho con caracteres cuasi absolutos que, definitivamente, nos puede dar lugar a que en el futuro, una persona sostenga que los antecedentes judiciales, es decir el record policial, donde se registran los crímenes o delitos que ha cometido una persona, como se refiere a datos personales de aquel individuo, diga que estos datos personales, en virtud de su derecho a decidir, decide que no sean públicos, que esa información se la mantenga con carácter de reservada. Nos parece gravísima esa declaratoria que se hace, de que una persona tendrá derecho a decidir, con el carácter de absoluto sobre sus derechos personales. Por lo tanto yo he propuesto en mi informe de minoría, que se agregue, «dentro de los límites que señale la ley»".[208]

El texto propuesto y revisado por la Mesa 1 tuvo como norte la conceptualización del derecho desde la perspectiva europea, en especial la española. Esto se evidencia en el informe de la Mesa 1 que, entre los anexos justificativos, incluía una descripción sencilla pero concisa de su naturaleza, derechos, deberes y principios, realizado por Juan Manuel Fernández López, magistrado y ex director de la Agencia de Protección de Datos.[209]

En la votación final, la redacción es modificada de tal forma que conforme señaló el delegado de la Mesa 1: "El numeral 18 [...] fue reformulado, estableciéndose el derecho a acceder y decidir sobre información y datos de carácter personal y a que estos sean protegidos. Además, de que para la recolección, archivo, procesamiento, distribución o difusión de esos datos, se requerirá la autorización del titular o la prescripción de la ley, cuando sea pertinente".[210] La norma original incluía *la prescripción de la ley* como límite a la autodeterminación informativa, pero el texto aprobado sustituyó esta frase por la *del mandato de ley*.

Ahora bien, la mayoría de las intervenciones que solicitaban establecer un límite a la autodeterminación informativa, en lugar de sustentarla mediante su ponderación con el derecho a un interés general preponderante, tal como se ha realizado, en la resolución emitida el 15 de diciembre de 1983 por el Tribunal Constitucional Federal alemán, formularon una propuesta equivocada, respecto de la naturaleza pública[211] de los datos personales.

Una de las intervenciones que desarrollan esta errónea interpretación se transcribe a continuación:

> Creo que hay un exceso en el artículo que se refiere al derecho a la protección de datos de carácter personal. No estoy de acuerdo con el literal a) que dice «El Estado garantiza el derecho a decidir sobre los datos personales». En realidad creo que si bien tenemos un importante margen de decisión sobre nuestros datos, especialmente sobre los datos que conciernen a nuestra vida íntima, a nuestra vida personal, pero existen otros actos que son

[208] Ibíd., 68.
[209] M. MOLINA CRESPO, Presidenta la Mesa 1 de la Constituyente de 2008, "Informe de la Mesa 1 sobre artículos aprobados para que sean sujetos a discusión de la Asamblea Constituyente de Ecuador de 2008 sobre Derechos Civiles, debido proceso, Derechos Políticos y Derecho a la Comunicación".
[210] ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 67], 171.
[211] "[...] efectivamente, nosotros tenemos derecho a acceder a nuestros datos, tenemos derecho a corregirlos si estos están errados, tenemos derecho, obviamente, a disponer sobre cierta información que está en el ámbito de lo privado, pero no aquella información que está dentro de lo público". ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 64], 67.

> públicos, por ejemplo registros de antecedentes personales, por ejemplo, registros de filiación, son datos públicos y no podríamos tener un derecho absoluto de nosotros, decidir que esos actos ya no sean públicos, que pasen a la privacidad, que pasen a la reserva o que sean destruidos, consagrar así con este carácter de derecho absoluto, el derecho de decidir, sobre los datos personales, nos parece que puede ser contraproducente, en lugar de afianzar un derecho tan importante, como es el derecho a una información efectivamente correcta y por ende, debemos tener el derecho a acceder a nuestros datos, derecho a solicitar rectificaciones y a que se mantengan en reserva, en privacidad estrictamente las cosas, que son privadas y personales, más no los datos públicos".[212]

Sin duda, se confundió la naturaleza privada, personalista e individualizada de los datos de carácter personal, manifestación de los derechos de libertad, del libre desarrollo de la personalidad, de los derechos de la personalidad y de su dignidad humana; con aquellos datos que, sin dejar de pertenecer a sus titulares, por disposición legal deben constar en ficheros accesibles al público, como si perdieran su origen y se transformaran en datos públicos en sí mismos, por la pertenencia a un determinado archivo estatal. El titular del dato de carácter personal no muta, menos aún se vuelve titular de este derecho el Estado, sino que por el contrario es un responsable, como lo es cualquier otro, pero además con una doble función pues no solo debe cumplir con sus obligaciones como responsable de un fichero de datos personales, sino que al mismo tiempo es garante de los derechos de las personas.

Los datos públicos son aquellos que pertenecen al sector público[213], el cual está obligado a publicitarlos para garantizar a los ciudadanos el ejercicio del derecho a la información pública, la transparencia y control de las actuaciones públicas. Por lo tanto, los datos de carácter personal no son datos públicos. Los datos siguen siendo personales solo que, por mandato de ley, deben incluirse en bases de datos accesibles al público; de tal forma que la ley regula su registro, archivo, procesamiento, distribución o difusión.

En resumen, la versión final del numeral 19 del artículo 66 de la CRE señala: "Art 66. Se reconoce y garantiza a las personas: [...] 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley".

Como se ha mencionado en varias ocasiones, la Constitución de 2008 es la primera que reconoce el derecho a la protección de datos personales en Ecuador, lo hace desde el enfoque europeo, con la voluntad de que cumpla un alto estándar de protección. La norma antes citada describe perfectamente uno de los contenidos esenciales del derecho, el relativo a la autodeterminación informativa. No solo prescribe el *acceso* a los datos, como constaba en su antecedente inmediato, el *habeas data*, tanto en la Constitución de 1978, codificada en 1996 como en la Constitución de 1998, sino la *decisión* sobre su información. En otras palabras, se reconoce la titularidad y voluntad de los sujetos respecto de cómo manejar sus datos

[212] Ibíd., [Acta No. 50], 172-3.
[213] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR [2008], "Artículo 225: El sector público comprende: 1. Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral y de Transparencia y Control Social. 2. Las entidades que integran el régimen autónomo descentralizado. 3. Los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado. 4. Las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados para la prestación de servicios públicos".

personales, de tal forma que sea un derecho en sí mismo, más que un instrumento para ejercitar su proceso de autoconstrucción de su personalidad en una sociedad.

Al no hacer una mención expresa sobre el tipo de formato en el que debían constar los datos personales, como se estilaba en sus antecedentes inmediatos (*habeas data* de 1996 y de 1998), se puede concluir que no solo se resguardarán los datos de las personas en su versión electrónica, sino que se protegerán cualquiera sea la naturaleza del soporte que los contenga, ya sea virtual o incluso material.

Además, el texto constitucional describe cada una de las fases del manejo de los datos personales: recolección, archivo, procesamiento, distribución o difusión. Entonces, se puede colegir que la titularidad de los datos no se pierde, aun si estos han sido tratados de cualquier forma por un tercero. Que los datos personales serán protegidos independientemente de si el responsable del fichero es el propio Estado porque el vínculo que une los datos con su titular es indivisible. Que es indispensable la voluntad o el mandato legal para que opere el tratamiento de la información personal.

La norma constitucional señala la consagración de uno de los principios estructurales del derecho a la protección de datos, esto es el consentimiento, que además para que sea considerado como tal, debe reunir la característica intrínseca de ser informado. Así, el titular ejercita su derecho a la autodeterminación informativa: a) cuando por su propia voluntad, autoriza a un tercero, la recogida y tratamiento de sus datos personales; y b) cuando se abstiene de entregar su información.

Ahora bien, en aplicación de un análisis de ponderación entre derechos individuales e intereses colectivos y generales, la norma señala que esta autorización puede ser suplida por la ley en aquellos casos expresamente señalados en ella.

En cuanto a los derechos ARCO,[214] el transcrito numeral 19 del artículo 66 de la CRE determina expresamente el *acceso y la decisión*. Entonces, se puede colegir que los otros derechos rectificación, cancelación y oposición así como aquellos contemplados en la vigente normativa española: supresión, transparencia e información, limitación del tratamiento y portabilidad, están inmersos en el término *decisión*, que involucra en sí mismo una serie de verbos rectores, así como en la siguiente frase del texto constitucional que dice: *así como su correspondiente protección*.

Esta amplitud en la forma de abordar los derechos de los titulares de los datos personales nos permite concluir que la rectificación, la cancelación o la oposición son parte de los derechos protegidos por la norma constitucional, porque sin duda son parte esencial del derecho a la protección de datos ya que solo por intermedio de ellos se puede producir su efectiva vigencia y eficacia real. Pero además, por la forma tan general en la que está dispuesta su redacción, permite reconocer como incorporados al texto también los principios de información, calidad, finalidad, seguridad, entre otros, como elementos cruciales para la protección de los datos personales.

[214] Conforme la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal española se consideran derechos ARCO: el acceso, la rectificación, la cancelación y la oposición. La vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales LOPD-GDD, mantiene el derecho de acceso, de rectificación y de oposición pero sustituye la denominación cancelación por supresión; además adiciona los derechos de transparencia e información, limitación del tratamiento y de portabilidad.

Los tradicionales derechos ARCO propios de la derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal española se encuentran igualmente desarrollados en el artículo 92 de la CRE que establece la garantía constitucional del *habeas data*, la cual se analizará en la parte pertinente de este trabajo doctoral.

4.2 Contenido esencial de los derechos fundamentales

Si bien, el contenido esencial es una de aquellas garantías constitucionales que tienen por finalidad la limitación del poder de aquellos entes creadores de normas, por su objetivo primario que busca el respeto a la sustancia de un derecho, puede ser usado también como método de investigación para delimitar un contenido que explicite los elementos mínimos que debe contener un derecho para diferenciarlo de otro similar o parte de una categoría o tipo común, otorgarle autonomía, independencia y volverlo eficaz porque un derecho adecuadamente delineado y conformado se convierte en salvaguarda real de los derechos de las personas.

En tal sentido, el objetivo de la presente investigación es determinar y analizar el contenido esencial del derecho a la protección de datos personales en los modelos europeo, norteamericano y latinoamericano, con la finalidad de identificar aquel régimen mayoritariamente afín a la normativa ecuatoriana, cuyos sistemas y reglas, así como principios y derechos deban incorporarse al ordenamiento jurídico ecuatoriano para una coherente protección.

Por tanto, se vuelve indispensable un acápite especial para, desde un enfoque constitucional, determinar el contenido esencial de un derecho. Toda vez que en el caso ecuatoriano la protección de datos personales se encuentra recogida como derecho de libertad en el numeral 19 del artículo 66 de la CRE. Anotándose que deberá dilucidarse el contenido esencial de este derecho a la luz de los principios establecidos en la mencionada Constitución.

4.2.1 Dimensiones en las que se salvaguarda el contenido esencial de un derecho

Los diferentes sistemas constitucionales han adoptado al contenido esencial como un mecanismo de cautela constitucional[215] o de límites al ejercicio de la soberanía[216] que garantiza el respeto de los derechos fundamentales, por parte de: a) legisladores, en su facultad de creación y delimitación de los derechos; b) jueces constitucionales, en su facultad

[215] "En conclusión, el efecto irradiador, la vinculación general, la eficacia directa y la garantía del contenido esencial aparecen como "el derecho de los derechos" en la medida de que dichas características hacen posible que hablemos de derecho fundamentales, o lo que es lo mismo, la inexistencia de aquellas conllevaría que hablemos de cualquier otra categoría, pero no derechos fundamentales en un Estado constitucional y democrático de derecho". Véase J. BENAVIDES ORDÓÑEZ Y J. ESCUDERO SOLIZ, edit., *Manual de justicia constitucional ecuatoriana* (Quito: Corte Constitucional del Ecuador, 2013), 96.

[216] "La condición de esenciales o fundamentales de los derechos en el Estado Constitucional implica la prevalencia de ellos sobre toda norma anterior o sobrevenida, en la medida que tales derechos constituyen un límite al ejercicio de la soberanía obligando a todos los poderes estatales como establece el inciso 2° del artículo 5°, pudiendo ser aplicados directamente ya que constituyen parte de la Constitución, y constituyendo criterios hermenéuticos preferentes en toda operación de creación o aplicación del derecho…". Véase H. NOGUEIRA ALCALÁ, "Aspectos de una teoría de los derechos fundamentales: la delimitación, regulación, garantías y limitaciones de los derechos fundamentales", *Revista Electrónica Ius et Praxis* 11, No. 2 (2005). ‹www.scielo.cl/iusetp.htm›.

interpretativa; y, c) en general del Ejecutivo[217] y de todo poder público creador y aplicador de derecho.[218] Por tanto, si lesiona el contenido nuclear de los derechos, su obra sería objeto de revisión constitucional, por medio de una acción de inconstitucionalidad,[219] por ejemplo. Dicho de otra manera, se protege a la regulación de un derecho fundamental como instituto (marco de una convivencia humana justa y pacífica STC25/1981),[220] de tal suerte que el legislador o el juez constitucional deberá respetar el contenido esencial a la hora de desarrollar y limitar los contornos de un derecho (teoría objetiva).[221] La positivización de un derecho fundamental en un texto constitucional se concreta mediante la tutela judicial efectiva y en especial del contenido esencial.[222]

El contenido esencial también tiene una manifestación subjetiva (teoría subjetiva). La categoría de núcleo esencial conlleva a la problemática de objeto de protección,[223] y al ejercicio real de esta facultad subjetiva, de tal forma que el Estado, las personas y colectivos en general deben respetar el contenido esencial de un derecho, y en caso de transgresión, el perjudicado puede interponer las acciones que correspondan.

Finalmente, estas dos teorías no son contrapuestas ni excluyentes, pues son consecuencia directa de las facetas o dimensiones naturales de los derechos constitucionales,[224] pues tanto la dimensión objetiva como la subjetiva obtienen de la institución del contenido esencial los elementos necesarios para la protección integral de un derecho fundamental.[225] Ahora bien, el contenido esencial no se limita a la norma constitucional sino que puede referirse a derechos subjetivos constitucionales o no.[226]

4.2.2 Concepto de contenido esencial

Una vez identificadas las esferas o dimensiones en las que se salvaguarda el contenido esencial de un derecho, resta comprender qué debe entenderse por *contenido esencial*. El Tribunal Constitucional español en sentencia STC 11/1981, de 8 de abril de 1981, señaló dos caminos posibles para aproximarse a la idea de contenido esencial.

a) El primer camino relativo a *la naturaleza jurídica o el modo de concebir o de configurar cada derecho:*

   Mediante el cual se propone establecer "una relación entre el lenguaje que utilizan las disposiciones normativas y lo que algunos autores han llamado el metalenguaje o ideas generalizadas y convicciones generalmente admitidas entre los juristas, los jueces y, en general, los especialistas en Derecho. [...] El tipo abstracto del derecho

[217] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR PARA EL PERÍODO DE TRANSICIÓN, [Sentencia No. 012-2009-SEP-CC], 20.
[218] H. NOGUEIRA ALCALÁ, HUMBERTO, "Aspectos de una teoría de los derechos".
[219] J. BENAVIDES ORDÓÑEZ Y J. ESCUDERO SOLIZ, edit., *Manual de justicia constitucional ecuatoriana*, 96.
[220] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 601.
[221] J. BENAVIDES ORDÓÑEZ Y J. ESCUDERO SOLIZ, edit., *Manual de justicia constitucional ecuatoriana*, 92-3.
[222] P. CRUZ VILLALÓN, "Formación y Evolución de los Derechos Fundamentales", *Revista Española de Derecho Constitucional* 25, (1989): 42.
[223] J. BENAVIDES ORDÓÑEZ Y J. ESCUDERO SOLIZ, edit., *Manual de justicia constitucional ecuatoriana*, 93.
[224] Los derechos constitucionales poseen dos facetas que actúan conjuntamente: la de constituir una pretensión jurídica de su titular (derecho subjetivo) y la de estar expresados en normas constitucionales que forman parte del ordenamiento jurídico (derecho objetivo), y, a la vez, ser normas constitucionales. Véase M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 601.
[225] J. BENAVIDES ORDÓÑEZ Y J. ESCUDERO SOLIZ, edit., *Manual de justicia constitucional ecuatoriana*, 93.
[226] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 11/1981].

preexiste conceptualmente al momento legislativo y en este sentido se puede hablar de una recognoscibilidad de ese tipo abstracto en la regulación concreta. Los especialistas en Derecho pueden responder si lo que el legislador ha regulado se ajusta o no a lo que generalmente se entiende por un derecho de tal tipo, [atendiendo para ello] al momento histórico de que en cada caso se trata y a las condiciones inherentes en las sociedades democráticas, cuando se trate de derechos constitucionales".[227] Este primer camino responde a la primera dimensión de salvaguarda del contenido esencial de un derecho que desde la teoría objetiva pretendía su efectividad y garantía atendiendo exclusivamente desde el respeto del ordenamiento jurídico por parte de los generadores normativos.

b) El segundo camino consiste en buscar "los intereses jurídicamente protegidos como núcleo y médula de los derechos subjetivos",[228] por el cual se señala que "Se puede entonces hablar de una esencialidad del contenido del derecho para hacer referencia a aquella parte del contenido del derecho que es absolutamente necesaria para que los intereses jurídicamente protegibles, que dan vida al derecho, resulten real, concreta y efectivamente protegidos. De este modo, se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección".[229] Asimismo, este segundo camino responde a una dimensión de salvaguarda del contenido esencial de un derecho desde la teoría subjetiva que consagra el respeto al contenido esencial en el ejercicio real de los derechos subjetivos de las personas. El autor Prieto Sanchís señala que "el contenido esencial de un derecho sería aquella parte del derecho que todavía queda en pie una vez que ha operado una limitación justificada o legítima, lo que en hipótesis podría conducir al sacrificio completo del derecho si la protección de algún bien constitucional en conflicto así lo recomendase".[230] Este concepto visibiliza esta postura pragmática por la cual, el contenido esencial aparece cuando un derecho se pondera en un conflicto real.

En definitiva, los dos caminos "no son alternativos, ni menos todavía antitéticos, sino que, por el contrario, se pueden considerar como complementarios, de modo que, al enfrentarse con la determinación del contenido esencial de cada concreto derecho pueden ser conjuntamente utilizados para contrastar los resultados a los que por una u otra vía pueda llegarse".[231]

Dicha visión coincide también con las dimensiones de protección del contenido esencial que en idéntico caso coexisten en garantía de una protección integral del derecho.

Al utilizar complementariamente los dos caminos propuestos, la misma sentencia española establece un concepto completo sobre contenido esencial, que consiste en "aquella parte del contenido de un derecho sin la cual éste pierde su peculiaridad o, dicho de otro modo, lo que hace que sea recognoscible como derecho perteneciente a un determinado tipo. Es también aquella parte del contenido que es ineludiblemente necesaria para que el derecho permita a su

[227] Ibíd.
[228] Ibíd.
[229] Ibíd.
[230] L. PRIETO SANCHÍS, "La limitación de los derechos fundamentales y la norma de clausura del sistema de libertades", *Derechos y libertades: revista del Instituto Bartolomé de las Casas*, No. 8 (2000): 438.
[231] España, TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 11/1981].

titular la satisfacción de aquellos intereses para cuya consecución el derecho se otorga".[232] Como se señala en la mencionada sentencia, un determinado contenido se considera esencial a un derecho si es que su ausencia produce su desnaturalización o que estemos frente a otro derecho.[233] Este concepto esbozado por el Tribunal Constitucional español ha sido incorporado en la jurisprudencia ecuatoriana mediante la sentencia No. 012-09-SEP-CC[234] que lo asume como propio.

Coincidente con esta posición jurídica, el Tribunal Constitucional español ampliamente influenciado por la doctrina alemana considera que "al constituir los derechos fundamentales y las libertades públicas, facultades ejercitables frente al Estado, el legislador puede limitarlas como mecanismo de defensa propia y de defensa respecto a los individuos".[235] De tal forma que existen dos niveles de comprensión del contenido esencial. Un nivel respecto a la descripción normativa del derecho y otro referente al ámbito de su efectiva y real aplicación en el caso concreto.

En la jurisprudencia colombiana, la Corte Constitucional, a razón de la determinación de que la ley estatutaria no debe regular todo evento ligado a derechos fundamentales, sino solo los elementos estructurales esenciales, para determinar cuáles son estos ha establecido lo siguiente:

> [...] la jurisprudencia constitucional se ha valido de la teoría del núcleo esencial, según la cual, los derechos fundamentales tienen: (i) un núcleo o contenido básico que no puede ser limitado por las mayorías políticas ni desconocido en ningún caso, ni siquiera cuando un derecho fundamental colisiona con otro de la misma naturaleza o con otro principio constitucional; y (ii) un contenido adyacente objeto de regulación. De conformidad con la jurisprudencia constitucional es competencia del legislador estatutario desarrollar aspectos importantes del núcleo esencial, siendo, asuntos importantes del núcleo esencial propios de leyes estatutarias: (i) la consagración de límites, restricciones, excepciones y prohibiciones de alcance general; y (ii) los principios básicos que guían su ejercicio. Otro elemento que puede deducirse a partir de un examen de la estructura de los derechos fundamentales es la definición de las prerrogativas básicas que se desprenden del derecho para los titulares y que se convierten en obligaciones para los sujetos pasivos.[236]

Finalmente, el autor Humberto Nogueira Alcalá añade un elemento adicional a la comprensión general del contenido esencial cuando señala que "la concepción de que los derechos y los límites no pueden entenderse como categorías diferentes. El contenido del derecho se conforma por el conjunto de atributos y facultades que representa como por las fronteras o límites que se distinguen respecto del ejercicio de tales derechos".[237] En el mismo sentido, Pérez y Barceló señalan que "para dar vida al bien jurídico de que se trate (objeto) el derecho proporciona al titular un haz de facultades, posibilidades de acción, garantías y medios (contenido). Este conjunto de poderes jurídicos que el contenido comprende ha de venir determinado por la Constitución y, como tal, no debiera poder ser restringido por la

---

[232] Ibíd.
[233] Ibíd.
[234] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR PARA EL PERÍODO DE TRANSICIÓN, [Sentencia No. 012-2009-SEP-CC].
[235] J. M. GOIG MARTÍNEZ, M. A. NUÑEZ MARTÍNEZ Y C. NUÑEZ RIVERO, *El sistema constitucional de derechos y libertades según la jurisprudencia del Tribunal Constitucional* (Madrid: Editorial Universitas Internacional S.L., 2006), 18.
[236] CORTE CONSTITUCIONAL DE COLOMBIA, [Sentencia C-748/11].
[237] H. NOGUEIRA ALCALÁ, "Aspectos de una teoría de los derechos fundamentales", 13.

intervención de ningún poder público (legislativo, ejecutivo o judicial)".[238] Dicho de otra manera, se vuelve indispensable determinar los límites de un derecho, de tal forma que, en los contornos se pueda establecer las diferencias con otros derechos y una posible desnaturalización cuando existan confusiones. Además, limitar la actuación de los poderes públicos que pueden privar de contenido esencial a un derecho y volverlo ineficaz e inútil.

En consecuencia, conforme se cita en líneas precedentes, la Corte Constitucional ecuatoriana considera el concepto de contenido esencial como aquella parte medular o nuclear de un derecho sin el cual este pierde su peculiaridad o particularidad que lo diferencia de otros similares y, en consecuencia, permite la satisfacción de las expectativas del titular que espera de él la defensa de los intereses que supone el derecho otorga.[239]

4.2.3 Delimitación de los derechos fundamentales atendiendo a su contenido esencial

Del análisis general de los elementos que conforman la estructura de los derechos que constan desarrollados en la Constitución de 2008 se determinan que son criterios fundamentales los siguientes: titular, objeto, contenido y sujeto pasivo u obligado. Esta estructura materializa el contenido esencial de un derecho y permite su configuración.

En la realidad normativa, la estructura de un derecho: titulares o sujetos activos, objeto o bien jurídico, contenido de las facultades que les corresponden a dichos titulares para el ejercicio de ese objeto y sujetos pasivos u obligados que deben facilitar a los mencionados titulares la libre disposición sobre dicho objeto o bien jurídico,[240] no necesariamente están completas, claras o unívocas, de tal forma que pueden suscitarse contradicciones o lagunas que pueden ser corregidas utilizando diversas formas de solución.

Una de esas formas de solución es la interpretación por la cual "los límites y el contenido de los derechos fundamentales hay que determinarlos en una visión de conjunto que los tome en cuenta como parte constitutiva de un conjunto global. Ninguna norma constitucional puede interpretarse solamente desde sí misma [...] Los contenidos esenciales de los particulares bienes jurídicos-constitucionales no están desvinculados los unos de los otros. Se determinan recíprocamente".[241] Así, se justifica y se vuelve indispensable una interpretación conjunta, por cuanto los bienes jurídicos recogidos en la Constitución se interrelacionan, se superponen, se contradicen siendo imperante una visión global para su correcta interpretación y aplicación.

Una forma visible de delimitación del contenido esencial de un derecho la puede realizar el legislador, cuando la propia norma constitucional le autoriza expresamente, en virtud del principio de reserva de ley.

Pero, no solo los legisladores sino los poderes públicos en general, desde sus distintas facultades pueden intervenir para generar, interpretar o concretar preceptos constitucionales que contienen derechos o garantías. Ya sea modificando la normativa en algunos de los elementos estructurales del derecho (titular, objeto, facultades, entre otros) y por cuanto

[238] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 610.
[239] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR PARA EL PERÍODO DE TRANSICIÓN, [Sentencia No. 012-2009-SEP-CC].
[240] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 601.
[241] P. HABERLE, *La garantía del contenido esencial de los derechos fundamentales en la ley fundamental de Bonn* (Madrid: Dykinson, 2003), 8 y 62.

pudiera afectarse el ejercicio del derecho, en este caso, es necesario que la Constitución lo autorice expresamente. O en su defecto, cuando se debe completar la configuración de un derecho, si el constituyente no lo ha hecho, determinando su contenido o fijando de la forma de su ejercicio, como sus garantías procesales.[242]

El proceso de delimitación de un derecho se concibe como el "establecer su contenido (haz de facultades, garantías y posibilidades de actuación) y sus fronteras o límites. En otras palabras, delimitar es determinar el ámbito de realidad protegido por el derecho lo que determina sus contornos. Para delimitar el contenido del derecho deben tenerse presente dos elementos: el identificar el ámbito de la realidad al que se alude y fijar lo que se entiende por éste; y el tratamiento jurídico contenido en el precepto que reconoce el derecho, fijando su contenido y el alcance que se da a su protección constitucional".[243] Es decir, la delimitación implica una configuración y descripción completa conforme a la estructura formal de la norma en una relación constitucional interdependiente,[244] así como su acoplamiento a un contexto real de aplicación de derechos.

Adicionalmente, en este proceso de delimitación se deben distinguir los derechos fundamentales desde su complejidad. Su delimitación puede realizarse desde la Constitución de forma directa cuando el derecho es elaborado. En otras ocasiones se requerirá un desarrollo legal para su exigibilidad y por ende su delimitación se complementará desde la legislación correspondiente, incluidos no solo los aspectos positivos de concreción, sino incluso "de los demás elementos que no se hallan en el texto constitucional como, en forma negativa, de las posibles restricciones que se hubieran podido introducir".[245]

En el proceso de delimitación de un derecho resta identificar los límites internos o inmanentes y los límites externos. Por medio de los *límites internos*, que no son restricciones o limitaciones al derecho sino que dependen de la propia estructura del derecho, pues son aquellos que identifican donde termina su contenido. De tal forma que identifican el conjunto de facultades que un derecho entraña y sus contornos o fronteras a partir de su construcción dogmática. Forman parte de la definición del contenido del derecho aunque sea desde una perspectiva negativa y por eso son delimitados, pues el derecho es lo que queda dentro de los límites inmanentes.[246] "Los límites inmanentes son los límites que se corresponden con el contenido esencial o cercan a este".[247]

Los segundos, son los *límites externos,* que operan como restricción al derecho en sí mismo por parte del poder público que lo reduce estructuralmente y que posibilitan la compatibilidad de los derechos entre sí y con los otros bienes constitucionalmente protegidos.[248] Por tanto, puede incluirse una restricción siempre que suponga la defensa de algún otro bien

[242] H. NOGUEIRA ALCALÁ, "Aspectos de una teoría de los derechos fundamentales", 36.
[243] Ver I. DE OTTO Y PARDO, 1988. "La regulación del ejercicio de los derechos y libertades. La garantía de su contenido esencial en el artículo 53.1 de la Constitución", en L. MARTÍN-RETORTILLO Y I. DE OTTO Y PARDO. *Derechos fundamentales y Constitución* (Madrid: Cuadernos Cívitas Derecho Constitucional). Ver también su otro libro, *Derecho Constitucional. Sistema de fuentes*, 2a. ed., (Madrid: Ed. Ariel Derecho, 1988, citado por Ibíd., 7).
[244] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit. *Curso de derecho constitucional*, 611.
[245] Ibíd.
[246] Ibíd.
[247] P. HABERLE, *La garantía del contenido esencial de los derechos fundamentales en la ley fundamental de Bonn*, 58.
[248] H. NOGUEIRA ALCALÁ, "Aspectos de una teoría de los derechos fundamentales: la delimitación, regulación, garantías y limitaciones de los derechos fundamentales".

constitucionalmente protegido. Por lo que, un derecho limitado es aquel que ha sido recortado en alguno de sus elementos fundamentales por alguna disposición externa.[249]

Consta también como criterio delimitador del contenido esencial de los derechos fundamentales, el de la dignidad humana, ya que "la dignidad ha de permanecer inalterada cualquiera que sea la situación en que la persona se encuentre [...] constituyendo, en consecuencia un mínimum invulnerable que todo estatuto jurídico debe asegurar".[250] "Sin embargo, se puede utilizarse solo excepcionalmente en aquellos derechos que ha sido referidos a ella [...] Debido al hecho de que esta resulta ambigua, apta para un entendimiento absoluto y relativo, lo que convierte a la dignidad de la personas en un referencia susceptible de ponderación"[251].

Definitivamente, el contenido esencial de un derecho se vulnera cuando el derecho queda sometido a limitaciones que lo hacen impracticable, o dificultan más allá de lo razonable o lo despojan de la necesaria protección.[252]

En conclusión, la delimitación del derecho fundamental que permite marcar o definir su contenido esencial es:

> [...] un proceso plural en que deben tenerse en cuenta una multiplicidad de factores articulados en torno a dos grandes categorías: por un lado, la configuración del contenido en sus distintas fases y, por otro lado, sus posibilidades de limitación; en otras palabras: la configuración del contenido como determinación de los elementos que forman parte del contenido (delimitación) y las restricciones que es el contenido así delimitado y que pueden sufrir en determinadas circunstancias (límites).[253]

4.2.4 Formas de restricción o interpretación de un derecho desde las teorías sobre el contenido esencial

Se ha realizado un análisis del proceso de delimitación de un derecho, resta estudiar las formas de restricción o de interpretación que pueden producirse respecto del contenido esencial de un derecho.

En un primer momento, estas varias formas de solución pudieran resultar antagónicas, pero pueden supervivir de forma armónica y complementaria y se conocen en la doctrina como teorías absoluta, relativa y mixta.

a) Teoría absoluta sobre el contenido esencial de los derechos

Esta teoría considera al contenido esencial de los derechos desde una visión normativa constitucional del derecho, de carácter estricto, de tal forma que plantea un régimen rígido, casi estático,[254] un núcleo resistente que debe ser preservado en todo caso, aun cuando concurriesen razones justificadoras de su limitación o restricción.[255] Esta posición se justifica

[249] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit. *Curso de derecho constitucional*, 611.
[250] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 120/1990], FJ 4.
[251] I. GUTIÉRREZ GUTIÉRREZ, *Dignidad de la persona y derechos fundamentales* (Madrid: M. Pons, Ediciones Jurídicas y Sociales, 2005), 110-6.
[252] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 11/1981].
[253] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 611.
[254] H. NOGUEIRA ALCALÁ, "Aspectos de una teoría de los derechos fundamentales", 438.
[255] L. PRIETO SANCHÍS, "La limitación de los derechos fundamentales", 438.

desde dos posturas: a) la que considera que no pueden limitarse los derechos fundamentales debido a que protegen intereses de particulares (Ekkehart Stein), y b) la que señala que la dignidad humana precautela el contenido esencial de los derechos, que consiste en una positivización de esta dignidad inafectable y del contenido inviolable de los derechos humanos (visión iusnaturalista)".[256]

De otro lado, se considera que el contenido constitucionalmente garantizado de un derecho "únicamente está compuesto por los poderes o facultades mínimos o esenciales que permiten la vida del derecho, se deducen todos ellos directamente de la Constitución y, en consecuencia, siempre son inatacables e inmodificables" .[257] Estas normas tienen entonces un "componente sustancial o núcleo duro, no disponible ante cualquier injerencia del poder público, aun cuando dicha intromisión persiga un fin legítimo y sea producto de una aplicación estricta del principio de proporcionalidad".[258]

La crítica a esta teoría, además de su obvia rigidez que por sí sola desconoce las variables aplicativas de un derecho, considera al núcleo duro de un derecho "como un círculo concéntrico cuya circunferencia constituye el límite o frontera que el legislador no puede traspasar nunca". Entonces, se plantean dos inquietudes, la primera respecto del anillo periférico que aparece como una zona de libre penetración para el legislador, que pudiera ser alterada aun de forma arbitraria e injusta. La segunda, la indefinición del "límite entre el núcleo duro de los derechos y los contenidos accesorios o periféricos de estos".[259]

La normativa constitucional ecuatoriana de 2008, en el artículo 11 numeral 4 señala: "El ejercicio de los derechos se regirá por los siguientes principios: [...] 4. Ninguna norma jurídica podrá restringir el contenido de los derechos ni de las garantías constitucionales". Para Benavides la redacción de la versión ecuatoriana de la cláusula de contenido esencial recoge la "influencia ejercida por el texto germano en el ibérico, así como la de este último, sobre el andino".[260] Entonces, se formula la imposibilidad absoluta de que se pueda restringir el contenido de un derecho, y además se añade en este marco de protección a las garantías constitucionales, porque son herramientas de tutela de derechos.

En el Título IX relativo a la Supremacía de la Constitución, Capítulo tercero, titulado Reforma de la Constitución, consta el artículo 441 de la CRE se señala que es posible enmendar uno varios artículos de la Constitución siempre que no se altere su estructura fundamental, o el carácter y elementos constitutivos del Estado, o que no se establezca restricciones a los derechos y garantías, o que no se modifique el procedimiento de reforma de la Constitución. En consecuencia, por disposición expresa de la Constitución no podría enmendarse lo relativo a derechos y garantías cuando se intente su limitación.

Asimismo, el artículo 442 que se refiere a la reforma parcial expresa: "La reforma parcial que no suponga una restricción en los derechos y garantías constitucionales, ni modifique el procedimiento de reforma de la Constitución tendrá lugar por iniciativa de la Presidenta o

[256] H. NOGUEIRA ALCALÁ, "Aspectos de una teoría de los derechos fundamentales".
[257] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 610-1.
[258] J. BENAVIDES ORDÓÑEZ Y J. ESCUDERO SOLIZ, edit., *Manual de justicia constitucional ecuatoriana*, 94.
[259] H. NOGUEIRA ALCALÁ, "Aspectos de una teoría de los derechos fundamentales".
[260] "[E]l artículo 19 de la Ley Fundamental de Bonn que establece en su número 2: «que en ningún caso se podrá afectar el contenido esencial de un derecho fundamental», así también el artículo 53, numeral 1 de la Constitución española, dispone que: «Sólo por ley, que en todo caso deberá respetar su contenido esencial podrá regularse el ejercicio de los derechos y libertades...»". J. BENAVIDES ORDÓÑEZ Y J. ESCUDERO SOLIZ, edit., *Manual de justicia constitucional ecuatoriana*, 92.

Presidente de la República...". Nuevamente, la norma constitucional impide la reforma parcial de la Constitución cuando esta pretenda restricciones a derechos y garantías.

Como vemos, tanto la cláusula que impide la limitación al contenido esencial de un derecho, que consta como principio que rige el ejercicio de los derechos en el artículo 11, numeral 4, de la Constitución; así como la imposibilidad de limitar, mediante enmienda o de reforma parcial los derechos y garantías, nos permite concluir que es criterio unívoco no permitir restricciones a los derechos fundamentales. Ante estas expresas exclusiones podríamos concluir, de primer momento, que la teoría aplicable en Ecuador es la absoluta.

A ese respecto, el constitucionalista ecuatoriano Agustín Grijalva señala que inicialmente podríamos pensar que no es posible, de ninguna manera, realizar limitaciones a los derechos fundamentales, en virtud de las prohibiciones descritas en los artículos analizados. No obstante, estas normas deben ser leídas desde una perspectiva integral en su interrelación con otros principios y bienes jurídicos constitucionales, en especial con el de progresividad y no regresividad de un derecho, pues el legislador justamente tiene por función regular, limitar o condicionar el ejercicio de estos derechos, como lo reconoce el artículo 11, numeral 3, inciso segundo de la misma Constitución; lo que no puede el legislador es restringir o invadir el contenido esencial de estos derechos.[261]

b) La teoría relativa sobre el contenido esencial de los derechos

Según la teoría relativa, el contenido esencial es el resultado de la ponderación de los derechos o del derecho respectivo con otros bienes jurídicos constitucionales.[262] En otras palabras, un derecho fundamental solo puede ser objeto de limitación válida desde un juicio de constitucionalidad si está justificada constitucionalmente mediante el juicio de razonabilidad y proporcionalidad y si no afecta el contenido esencial de los derechos.[263]

No tiene sentido buscar el núcleo duro de cada derecho fundamental y la parte accidental, como en la teoría absoluta, ya que el contenido esencial no es intocable sino que es más bien fruto de una argumentación que se produce ante el escenario de colisión entre derechos. Por tanto, el contenido esencial vendría a ser lo que queda del derecho luego de aplicar la técnica de la ponderación. También podemos definirlo, siguiendo a Manuel Medina Guerrero, como aquella parte del derecho que empieza cuando el límite deja de ser proporcionado.[264] Y por ende, el contenido esencial del derecho sería en sí mismo indeterminado, pues cada caso específico determinaría el derecho.[265] Se justifica en la búsqueda de proteger el derecho en toda su extensión, por medio de un equilibrio entre los derechos de las personas y los intereses de la sociedad (bien común).[266]

En el caso del Ecuador, el único facultado para realizar un proceso de ponderación o de interpretación jurídica de la propia Constitución, que está obligado a desarrollar el contenido esencial de un derecho, al verificar que no se violen derechos constitucionales, y por el contrario los concreten, desarrollen y regulen es la Corte Constitucional. Para tal efecto, será

[261] A. GRIJALVA, "Interpretación constitucional, jurisdicción ordinaria y Corte Constitucional", en *La nueva Constitución del Ecuador: Estado, derechos e instituciones* (Quito: Corporación Editora Nacional, 2009), 278.
[262] H. NOGUEIRA ALCALÁ, "Aspectos de una teoría de los derechos fundamentales", 27.
[263] Ibíd., 35.
[264] J. BENAVIDES ORDÓÑEZ Y J. ESCUDERO SOLIZ, edit., *Manual de justicia constitucional ecuatoriana*, 94.
[265] H. NOGUEIRA ALCALÁ, "Aspectos de una teoría de los derechos fundamentales", 25.
[266] Ibíd., 27.

indispensable que se apliquen los principios contenidos en el artículo 11, en especial el numeral 4 que se refiere a la garantía de no restricción de un derecho o de un garantía constitucional (contenido esencial),[267] y el numeral 8 relativo al principio progresividad y de no regresividad de los derechos.[268]

Por último, la mayor crítica a la teoría relativa parte del enfoque que se hace del contenido esencial del derecho, extremadamente variable e insegura, puesto que, "el contenido esencial del derecho, se confunde con la ponderación de derechos, el que pasa a ser el único límite del legislador, con lo que se desfigura el contenido esencial de cada derecho, estableciendo una jerarquización concreta que depende de una valoración subjetiva del intérprete que puede variar de contenido un derecho".[269] Por esta causa, los derechos se relativizan, pues dependen de su valoración en relación de los demás bienes jurídicos constitucionalmente protegidos.[270] Prieto Sanchís llega a afirmar que el concepto de contenido esencial de los derechos se constituye así, en la teoría relativa, no solo en un "concepto indeterminado, sino más bien en un concepto impredecible";[271] de tal forma, que esta doctrina ampliamente criticada no es admisible por sí sola.

c) La teoría mixta sobre el contenido esencial de los derechos

De las deficiencias de las anteriores teorías aparece una posición intermedia que recoge ambas interpretaciones y conjuga reglas con principios. Toda limitación a un derecho fundamental debe conllevar la debida justificación, debiendo respetar además, en todos los casos su contenido esencial; dicho de otro modo, recoge "la fuerza vinculante de las reglas, y por otro lado, en que sostiene una suerte de sistema cerrado, es decir la posibilidad a que siempre hay principios a los que se puede acudir, y con ello no existe caso que no pueda ser resuelto sobre la base de planteamientos jurídicos, con ello el problema de las lagunas según Alexy ingresa en el ámbito de los solucionable".[272]

Conforme consta de la sentencia No. 012-09-SEP-CC, la teoría adoptada en Ecuador es la mixta, ya que recoge elementos absolutos como la visión normativa del derecho, la identificación de su núcleo duro inamovible; así como, elementos relativos como la ponderación de derechos, a la luz de una interpretación armónica, dirigida al fundamento y esencia misma de la norma; concretamente, una interpretación teleológica y sistemática aplicada a los derechos fundamentales, evitándose la depreciación del valor axiológico de los derechos fundamentales.[273] Sin embargo, Agustín Grijalva sostiene:

---

[267] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR [2008], "Artículo 11: El ejercicio de los derechos se regirá por los siguientes principios: [...] 4. Ninguna norma jurídica podrá restringir el contenido de los derechos ni de las garantías constitucionales".

[268] Ibíd., artículo 11: "El ejercicio de los derechos se regirá por los siguientes principios: [...] 8. El contenido de los derechos se desarrollará de manera progresiva a través de las normas, la jurisprudencia y las políticas públicas. El Estado generará y garantizará las condiciones necesarias para su pleno reconocimiento y ejercicio. Será inconstitucional cualquier acción u omisión de carácter regresivo que disminuya, menoscabe o anule injustificadamente el ejercicio de los derechos".

[269] H. NOGUEIRA ALCALÁ, "Aspectos de una teoría de los derechos fundamentales".

[270] Ibíd.

[271] L. PRIETO SANCHÍS, LUIS, "La limitación de los derechos fundamentales", 439.

[272] J. BENAVIDES ORDÓÑEZ Y J. ESCUDERO SOLIZ, edit., *Manual de justicia constitucional ecuatoriana*, 90.

[273] "[L]a teoría del contenido esencial: núcleo duro de derechos. El Contenido esencial consiste en una interpretación dirigida al fundamento y esencia misma de la norma; concretamente, una interpretación teleológica y sistemática aplicada a los derechos fundamentales. Se trata de buscar las formas de compatibilidad que respeten el núcleo central de cada uno de los derechos, solucionando, del modo más ajustado posible, la controversia y evitando que se vea frustrado el ejercicio legítimo de alguno de ellos. Esto se consigue

> [...] este tipo de jurisprudencia constitucional es más bien escasa en el Ecuador. Las resoluciones del Tribunal Constitucional casi no abordan la delicada tarea analítica de precisar o concretar jurídicamente los contenidos esenciales de los derechos que la Constitución establece, es decir los límites y parámetros que marcan la libertad de configuración del legislador. Tampoco se halla en esa jurisprudencia el uso de métodos modernos de interpretación constitucional, tales como la ponderación o los test de razonabilidad y proporcionalidad, orientados a evaluar la constitucionalidad de las regulaciones a los derechos constitucionales creadas mediante ley por el legislador y el Ejecutivo.[274]

Un caso emblemático de referencia, se produjo con las reformas al Código de Procedimiento Penal que introdujeron la detención en firme. Estas normas legales violaron aspectos esenciales del derecho constitucional al debido proceso tales como: la presunción de inocencia, el plazo razonable y, por otra parte, el propio derecho a la libertad.[275] Por lo que, pese a que la teoría visiblemente aplicable en Ecuador es la mixta, no obstante la práctica pudiera no ser del todo eficaz ante la falta de actuación del órgano responsable: Corte Constitucional.

4.3 Contenido esencial del derecho a la protección de datos personales

La búsqueda del contenido esencial del derecho a la protección de datos personales comenzará con la delimitación de sus límites internos y externos, y de su interrelación con otros derechos conexos, que incluso pertenecen al mismo grupo de derechos de la personalidad, y con los cuales tradicionalmente pueden suscitarse confusiones aparentes.

Sobre la perspectiva estructural del contenido esencial, se realizará un análisis desde la estructura prevista en la propia Constitución; así, en primer lugar aquellos presupuestos como el concepto de dato, luego la determinación de los titulares o sujetos activos, posteriormente el objeto o bien jurídico. En acápite aparte, el contenido de las facultades que les corresponden a dichos titulares. Finalmente, los sujetos pasivos u obligados.

Con la finalidad de determinar el contenido esencial del derecho a la protección de datos en el Ecuador y conforme al modelo planteado, se estudiará la naturaleza jurídica o el modo de concebir o configurar el derecho por parte de la doctrina, la normativa y la jurisprudencia que se considera de estándar adecuado.

En un segundo momento se identificarán los intereses jurídicamente protegidos como núcleo y médula de los derechos subjetivos; para tal efecto, es necesaria la búsqueda de sentencias de la Corte Constitucional que establezcan orientaciones generales y, principalmente, precedentes jurisprudenciales obligatorios. Después, se revisará la delimitación del contenido esencial del derecho desde el análisis de la propia norma constitucional y las limitaciones que pudieran estar autorizadas por el principio de reserva de ley. Más adelante, se revisará si existen normas legales dictadas por los poderes públicos en general, pero solo aquellos de aplicación general. Los textos legales de carácter sectorial, por su especificidad, se analizarán en el capítulo quinto de este trabajo doctoral.

---

concibiendo a los derechos no como pretensiones abstractas e individualistas, sino como facultades orientadas por un determinado fin que se da en el marco de la convivencia social". Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR PARA EL PERÍODO DE TRANSICIÓN, [Sentencia No. 012-2009-SEP-CC],.

[274] A. GRIJALVA, "Interpretación constitucional, jurisdicción ordinaria y Corte Constitucional", 279.

[275] Ibíd., 279-80.

Finalmente, se verificará si el derecho constitucional a la protección de datos personales ha sido limitado desde una teoría mixta; es decir, se realizará la identificación de su núcleo duro inamovible; así como, sin procurar una ponderación, por cuanto para este método de interpretación se necesita la colisión de derechos en un caso concreto, se realizará una interpretación teleológica, sistemática y armónica dirigida al fundamento y esencia misma del derecho.

4.3.1 Presupuesto del derecho fundamental: el concepto de dato personal

El vertiginoso avance de las tecnologías de la información y la comunicación provocan en las sociedades nuevas formas de transgresión de derechos fundamentales; por tanto, es indispensable avanzar con precisión y celeridad en la configuración de nuevos derechos o en el reconocimiento de distintos y nuevos contenidos o enfoques de aquellos derechos existentes. Pero además, y no menos importante, que las garantías constitucionales y legales que los tutelan vayan acoplándose a estos nacientes derechos, o a sus nuevos dimensionamientos, de tal manera que pueda perfeccionarse paulatinamente un adecuado sistema de protección.

Conforme consta en el numeral 19, del artículo 66 de la Constitución de la República del Ecuador (CRE), el presupuesto del derecho a la protección de datos personales es *el dato y la información de carácter personal*. Sin embargo, es necesario identificar si los criterios de protección descritos en la acción de *habeas data* y que constan en el artículo 92 de la CRE son pertinentes para proteger el derecho a la protección de datos personales o deben adaptarse a la naturaleza de este derecho fundamental.

Para aclarar esta temática, se vuelve indispensable identificar los conceptos de *datos e información de carácter personal*, para luego contrastarlos, asimilarlos, integrarlos o excluirlos de aquellos conceptos descritos en el mencionado artículo 92 de la CRE: *documentos, datos genéticos, bancos o archivos de datos personales e informes sobre sí misma, o sobre sus bienes*.

4.3.1.1 Antecedentes del derecho a la protección de datos personales

El derecho a la protección de datos personales tiene su origen en la intimidad, derecho del que se separa paulatinamente hasta que se le reconoce su autonomía mediante la jurisprudencia y posteriormente de la incorporación de normativa constitucional, legal e incluso reglamentaria. Tiene su evidente nacimiento en un mundo tecnificado y globalizado, en el que el ingente procesamiento de datos personales, la generación de sistemas y procesos de decisión y valoraciones automatizadas, así como la elaboración de perfiles completos de las personas provocan transgresiones no solo a la privacidad, sino a su autodeterminación informativa; es decir, a la titularidad y voluntad de los sujetos respecto de cómo manejar sus datos personales con miras a desarrollar un proceso de autoconstrucción de su personalidad en sociedad, y además replicar las consecuencias de valoraciones indeseadas, no autorizadas, equivocadas o inexactas o que pudieran afectar el ejercicio de otros derechos fundamentales.

Por eso, la necesidad de proteger todos los datos relativos a las personas:

> [...] no son algo anecdótico, sino que representan el registro de su vida, reflejan sus características, sus opciones vitales, sus debilidades. El tratamiento adecuado de los datos

> personales es una exigencia de la dignidad de la persona y del libre desarrollo de la personalidad, algo especialmente necesario en la etapa de desarrollo de la personalidad, de formación del carácter y de los valores personales. El conocimiento por parte de otros, de una información que una persona no ha querido revelar afecta seriamente a la forma en que ésta se desenvuelve normalmente en la sociedad, la manera en que es vista por sus familias, por sus vecinos, por sus compañeros de trabajo.[276]

Los avances tecnológicos han permitido la difusión masiva de datos e información y, en consecuencia, son exponenciales los daños a los derechos fundamentales.

Inicialmente el derecho a la protección de datos personales, por su antecedente inmediato con el derecho a la intimidad, atendía solo datos considerados íntimos, e incluso a aquellos que tenían un nivel adicional de protección, los denominados datos sensibles, esto es aquellos que "permitan identificar a la persona, confeccionando su perfil ideológico, racial, sexual, económico, o de cualquier otra índole".[277] Sin embargo, también se resguardan aquellos datos considerados irrelevantes, ya sean estos pasados, presentes e incluso futuros, ya que mediante su recopilación, almacenaje y tratamiento paulatino, pueden asociarse para entregar perfiles completos de las personas. De modo que no importa si los datos parecieran "«a priori irrelevantes, pueden servir para una finalidad diferente y, por lo tanto, proporcionan claves insospechadas sobre la persona». Le teoría del mosaico pone de relieve como datos aparentemente inocuos pueden aportar una información preciosa a la hora de elaborar un determinado perfil personal. Por tanto, todos aquellos datos referentes a la persona merecen la protección que otorga la Ley".[278]

Es fundamental anotar que, en cualquier caso, no se protegen los datos en sí mismos, sino a los titulares de esos datos. El objeto de resguardo del derecho a la protección de datos personales es la autodeterminación informativa, por la cual todos los ciudadanos tienen la libertad de decidir sobre sus datos, cualquiera sea la naturaleza de estos; dicho de otra manera, no solo aquellos referidos al ámbito de su intimidad o privacidad, sino todos los datos que aparentemente inocuos, mediante tratamiento sencillos, de procesos automatizados o incluso de minería de datos, pueden otorgar perfiles de personalidad y ser usados para violentar otros derechos fundamentales.

Debe atribuirse mayores niveles y garantías de protección a los datos personales; "es conveniente insistir en que la protección de datos personales es también un instituto de garantía de otros derechos fundamentales"[279] ya que la influencia y repercusión de la recopilación, tratamiento y difusión de los datos personales afectan directamente el ejercicio de las libertades individuales en una sociedad en la que lo virtual y lo real se interrelacionan constantemente.

---

[276] A. TRONCOSO REIGADA, *La protección de datos personales: en busca del equilibrio* (Valencia: Tirant lo Blanch, 2010), 32.
[277] C. CONDE ORTIZ, *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad* (Madrid: Dykinson, 2005), 66.
[278] M. L. FERNÁNDEZ ESTEBAN, *Nuevas tecnologías, Internet y derechos fundamentales* (Madrid: MacGraw-Hill, 1998), 129.
[279] A. TRONCOSO REIGADA, *La protección de datos personales*, 37.

4.3.1.2 Naturaleza jurídica del dato personal como presupuesto generalizado del derecho a la protección de datos personales

Una vez determinado que el derecho a la protección de datos personales protege no solo al dato íntimo o privado, sino también al inocuo, es necesario establecer la naturaleza jurídica del dato y de la información personal, para lo cual se recurrirá como referente inmediato a la Unión Europea con énfasis en España, ya que por intermedio de su Tribunal Constitucional y de su Agencia de Protección de Datos Personales[280] es la líder en los principales avances en el contenido esencial, manejo práctico y eficacia real de este derecho.

a) *Concepto de datos de carácter personal:* La Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en el artículo 2 relativo a las Definiciones, señalaba que: "A efectos de la presente Directiva, se entenderá por: a) «datos personales»: toda información sobre una persona física identificada o identificable". Coherente con la concepción jurisprudencial y doctrinaria, el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, *de Protección de Datos de Carácter Personal* (en adelante LOPD española), que es manifestación expresa de la Directiva europea antes citada, señalaba como definición de datos de carácter personal a "cualquier información concerniente a personas físicas identificadas o identificables". Asimismo, el artículo 5, literal f del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (en adelante Reglamento a la LOPD española), al determinar las definiciones aplicables decía que: "Definiciones. 1. A los efectos previstos en este reglamento, se entenderá por: f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".

   Actualmente, toda esta normativa ha sido sustituida por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos en adelante, (RGPD) y por el que se deroga la Directiva 95/46/CE, cuyo artículo 4 define al dato como "toda información sobre una persona física identificada o identificable («el interesado»)".

   Tradicionalmente se consideraba que solo ameritaba protección la información y no el dato, ya que "la información hace referencia, pues, a datos estructurados y seleccionados para un usuario, una situación, un momento y un lugar. Mientras no sean evaluados o aplicados a un problema específico, los datos seguirán siendo sólo datos, es decir, símbolos con poco o ningún significado".[281] Dicho de otro modo, se consideraba que el dato "no explica el porqué de las cosas y en sí mismo no significa nada [...] [mientras que] la información es el significado que una persona le asigna a un dato".[282]

[280] Ibíd., 2.
[281] R. H. SAROKA, *Sistemas de información en la era digital* (Buenos Aires: Fundación Osde, s.f), citado por A. PARDINI, "La información y su sistema de protección", *DeCITA 5/6.2006 Revista de direito do comércio internacional temas e atualidades Internet, comércio eletrônico e sociedade da informação* 5/6 (2006): 21.
[282] Ibíd.

Sin embargo, esta visión se encuentra superada pues se protege al dato porque de él se extrae información; por eso, las normas que regulan el derecho a la protección de datos personales conceptualizan al dato como información. En consecuencia, este derecho resguarda toda posible vulneración que puede producirse, no solo respecto de la información de un individuo sino de sus datos o incluso de fragmentos de datos, que por medio de procesos de tratamiento puedan trazar perfiles completos de una persona. Es decir, se protege al dato por la sola posibilidad de que pueda llegar a tener una significación, esto es convertirse en información.

Las normas citadas utilizan la frase *cualquier* dato o información, o la generalización *todo* tipo de información o dato, señalando que no queda por fuera ningún tipo de dato o soporte físico o virtual.

Por lo tanto, podemos señalar que se considera dato personal a toda información numérica, alfabética, también imágenes (gráfica y fotográfica), acústica (sonidos y voces) o cualquier otro de tipo de información con las condiciones de que puedan ser recogidas, registradas, tratadas o transmitidas, y de que pertenezcan a una persona física identificada o identificable. Anotándose que no solo se refiere a datos habituales o comunes, sino incluso aquellos que la persona desconozca sobre sí misma,[283] debido a la existencia de tratamientos como la minería de datos.

b) *Dato identificativo o identificable:* Conforme señala el artículo 2 literal a) de la Directiva 95/46/CE se consideran datos personales "toda información sobre una persona física identificada o identificable («el interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural y social".

Por su parte, el RGPD determina hoy en día, en su artículo 4, que "se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

En conclusión, son datos identificativos aquellos que permiten una atribución directa como nombres, dirección, teléfono, DNI; pero también aquellos que "se pueden sumar a los identificativos para someterlos a tratamiento [...] datos de características personales, datos de circunstancias sociales, datos académicos y profesionales, datos de detalles de empleo, datos de información comercial, datos económicos-financieros, datos de transacciones y datos especialmente protegidos".[284]

En cambio, son datos identificables aquellos que para los que no es "imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados y para determinar si una persona es identificable, hay que considerar el conjunto de los

[283] I. DAVARA FERNÁNDEZ DE MARCOS, *Hacia la estandarización de la protección de datos personales: propuesta sobre una «tercera vía o tertium genus» internacional* (Madrid: La Ley, Las Rozas, 2011), 141.
[284] D. SANTOS GARCÍA, *Nociones generales de la Ley orgánica de protección de datos y su reglamento: adaptado al RD 1.720/2007 de 21 de diciembre*, 2a. ed. (Madrid: Tecnos, 2012), 42.

medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona".[285]

Recomendaciones del Consejo de Europa señalan además que una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas. Si una persona natural no fuere identificable, los datos se considerarán anónimos.[286] Si bien, estos conceptos resultan ambiguos se puede concluir naturalmente que "no es lo mismo que se identifique a una persona utilizando criterios de búsqueda en el marco de un sistema automatizado, que a través de los documentos, que se disponga en soporte papel".[287]

Asimismo, si los datos se someten a un proceso de disociación, por el cual no es posible su asociación o identificación con su titular o afectado, se pierde la característica fundamental de su vinculación personal y se vuelven anónimos. Por lo tanto, los datos personales anonimizados dejan de estar bajo la égida del derecho a la protección de datos personales porque "cualquier información, en cuanto asociada a un titular, es información de carácter personal, no por la información en sí, sino por su asociación con la persona física a la que se protege".[288] Tal y como se establece expresamente en el Considerando 26 RGPD, "los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación".

Así pues, los datos o información se protegen por su vinculación con una persona. Esta vinculación puede ser directa (datos identificativos) o indirecta (datos identificables), pero es indispensable porque se protege la autodeterminación informativa de la persona.

c) *Casos especiales de datos personales:* Existen cierto tipo de datos, que por sus características no se tiene la certeza de su condición de personales, y en consecuencia debe analizarse si deben o no ser regulados. Toda vez que pueden ser considerados como mensajes de datos y existen dudas respecto de su vinculación a un individuo. Por ejemplo: la dirección de correo electrónico, *web* e *IP*, los *log-in* de acceso, los SMS, los datos de los fallecidos, del *nasciturus*. Asimismo, existe un grupo de datos de los que no existe dudas respecto de su naturaleza, sino que sus elementos definitorios determinan la necesidad de un régimen de protección blindado, como por ejemplo: datos sensibles, datos genéticos, datos de salud, datos obtenidos en sistemas de videovigilancia, entre otros.

[285] SAN recurso 948/2000, de 8 de marzo del 2002.
[286] CONSEJO DE EUROPA, [Recomendación No. R(97) 18 y exposición de motivos del comité de ministros a los estados miembros relativa a la protección de datos de carácter personal, recogidos y tratados con fines estadísticos], 3.
[287] J. ZABÍA DE LA MATA Y I. M. AGÚNDEZ LERÍA, edit., *Protección de datos: comentarios al reglamento* (Valladolid: Editorial Lex Nova, 2008), 112.
[288] I. DAVARA FERNÁNDEZ DE MARCOS, *Hacia la estandarización de la protección de datos personales*, 147.

a. *Correo electrónico:* En cuanto a considerar de carácter personal ciertos datos como la *dirección de correo electrónico*, incluso del institucional,[289] la Agencia Española de Protección de Datos (AEPD) ha señalado que tanto si la dirección está formada por el nombre y apellido de un titular, como si está formada por caracteres que permiten la personalización del e-mail, es obvio que contienen en sí mismos datos personales. En el mismo sentido ha razonado Zabía de la Mata respecto de los *nombres de dominio en Internet*,[290] aunque la AEPD aún no se ha pronunciado sobre el tema. En el caso del correo electrónico aun cuando de la simple lectura de la dirección de correo electrónico no se pueda obtener una identificación inicial de a quién pertenece el correo también será considerado dato personal cuando "la dirección necesariamente aparecerá referenciada a un dominio concreto, de tal forma que podrá procederse a la identificación de su titular mediante la consulta del servidor en que se gestione dicho dominio, sin que ello pueda considerarse que lleve aparejado un esfuerzo desproporcionado por parte de quien procede a la identificación".[291]

b. *Las dirección IP:* Respecto de la *dirección IP* tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal por cuanto existen muchas posibilidades de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como *cookies* con un identificador único o sistemas modernos de minería de datos unidos a bases de datos con información sobre usuarios de Internet que permitan su identificación.[292]

c. *Los log-in de acceso:* Acerca de los *log-in* de acceso a Internet o a páginas personales se consideran datos de carácter personal, si se identifica de forma directa al usuario. Por el contrario, si este es anónimo, en principio no sería un dato de carácter personal, pero si por ejemplo el proveedor de servicios de Internet, mediante ese *log in*, puede identificar al usuario con el que tiene un contrato de acceso a Internet, sí será considerado como un dato de carácter personal.[293]

d. *Los SMS:* Lo mismo ocurre con los *SMS*, "mensajes cortos remitidos por teléfono móvil, que se almacenan junto con el número del llamante, constituyen en sí mismo datos personales, de acuerdo con la definición incluida en la LOPD, que comprende «cualquier información concerniente a personas físicas o identificables»"[294].

---

[289] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Carácter de dato personal de correo electrónico institucional. Informe 0437/2010", 1.
[290] J. ZABÍA DE LA MATA Y I. M. AGÚNDEZ LERÍA, edit., *Protección de datos,* 115.
[291] AEPD 00377/2005, de 13 de junio.
[292] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Carácter de dato personal de la dirección IP. Informe 327/2003", 1.
[293] Ibíd.
[294] C. ALMUZARA ALMAIDA, *Estudio práctico sobre la protección de datos de carácter personal*, (Valladolid: Lex Nova, 2007), 131.

Si el mero hecho de disponer de ese número telefónico permitiría al destinatario del mensaje determinar quién ha manifestado una determinada preferencia al votar, sin más que telefonear a ese número [...]".[295]

e. *El Clic:* En el mundo empresarial la utilización de páginas web para informar, negociar o realizar publicidad es habitual. El cliente ingresa y navega en la página web y activa los faros de programación en *HTML o XML* mediante cada uno de los clics que realiza y que se graban en tarjetas de perfil y visita[296] con su nombre, que permite que los datos constantes en ellos le sean atribuibles. La serie de clics que utiliza para navegar en la página van dejando su rastro, el cual sometido a un tratamiento[297] permite definir su perfil económico, social, sus comportamientos de compra, su estado de ciclo de vida, etc. Es decir, el cliente entrega al *software* instalado en la página, datos de altísimo valor pues contestan las preguntas más importantes: ¿Qué quiere comprar y por qué?, lo cual permite implementar modelos de segmentación y de tarjetas de calificación de clientes a velocidades descomunales, y que simulan una interacción con el cliente mientras está de visita en la página web, pues le sugirieren productos de compra relacionados con el objeto de su búsqueda (ventas cruzadas). Por tanto, todos los datos que se capturen e ingresen en los ficheros (bases de datos), dentro de este tratamiento de dato, también se los considera de carácter personal.

d) *Datos de nasciturus:* Sobre los datos relativos a los *nasciturus* o concebido y no nacido, por no ser considerado persona sino sujeto de derechos, no es titular sino únicamente de aquellos derechos que la normativa expresamente le reconoce. Sin embargo, desde la perspectiva de la titularidad de los datos de la madre o de un grupo familiar los datos podrían tener protección.[298]

e) *Datos de fallecidos:* Respecto de los datos de los fallecidos, la AEPD estableció que al terminar la existencia legal de una persona no era posible que sus familiares o herederos interpusieran en su nombre derechos ARCO, sino que "tendrá por objeto comunicar al responsable la inexactitud del contenido del fichero, debiendo proceder a la cancelación de los datos correspondientes al fallecido"[299] en cumplimiento del principio de calidad de los datos. No obstante, actualmente el artículo 3 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en adelante LOPD-GDD, determina claramente que "las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos

[295] Comité Consultivo de la AEPD, "Conclusiones y recomendaciones efectuadas en la Inspección Sectorial relativa a Concursos Juegos y Sorteos de Televisión", *La protección de datos de Carácter Personal en España: Análisis y valoración*, 145.
[296] Pequeños ficheros electrónicos.
[297] España, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Artículo 3.- "Definiciones**:** A los efectos de la presente Ley Orgánica se entenderá por: [...] c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".
[298] M. VILLASAU SOLANA Y M. Á. VILA MUNTAL, "Intimidad y datos personales en Internet", en M. PEGUERA POCH, edit., *Principios de derecho de la sociedad de la información* (Navarra: Thomson Reuters-Aranzadi, Cizur Menor, 2010), 166.
[299] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Informe Jurídico 61/2008".

podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión. Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante".

f) *Datos de salud:* Son "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud" (artículo 4.15 RGPD). Con mayor precisión, el considerando número 35 del RGPD determina que, entre los datos personales relativos a la salud, se deben incluir "todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (9); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro".

g) *Datos genéticos:* Según el artículo 4.13 RGPD, se trata de datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

   Comprendido que los datos genéticos son distintos a las muestras biológicas por cuanto los primeros están constituidos por "información que puede obtenerse del análisis del mapa genético de una persona, y las segundas son las muestras de materia orgánica que son susceptibles de ser analizadas genéticamente. [...] la muestra biológica sin analizar no puede ser considerada como un dato, puesto que es necesario su análisis para la obtención de la información. En consecuencia, el mapa genético o resultado del análisis genético y las conclusiones que pueden obtenerse del estudio de dicho mapa deben considerarse datos personales cuando consten en algún medio que permita su lectura, estudio y comparación informatizado o no, esto es, que permitan su recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".[300] Esta innovación del reglamento responde a la incertidumbre generada por la complejidad de estos temas en los que se incluye también la identificación de si los datos genéticos son considerados datos de salud, lo que no afecta que sean datos íntimos que ameritan mayor protección.

[300] J. APARICIO SALOM, *Estudio sobre la protección de datos* (Cizur Menor, Navarra: Aranzadi, 2013), 126 a129., *Estudio sobre la protección de datos* (Cizur Menor, Navarra: Aranzadi, 2013), 126-129.

h) *Datos contenidos en sistemas de videovigilancia:* Los actuales sistemas de videovigilancia son considerados ampliamente invasivos, ya que permiten "la captación, y en su caso la grabación, de información personal en forma de imágenes".[301] Respecto de aquellas imágenes utilizadas por Fuerzas o Cuerpos de Seguridad, por justificarse la finalidad pública o el interés general, tienen un régimen especial que consta en normativas especializadas que los autorizan y regulan expresamente. En cambio, aquellas imágenes captadas, transmitidas, conservadas, o almacenadas en sistemas de videograbación, incluida la reproducción o emisión en tiempo real, que sean utilizadas para prevenir problemas de seguridad respecto de bienes y personas o para controlar actividades laborales, entre otros, cuyos responsables sean personas naturales y jurídicas, respecto de personas identificadas e identificables, se consideran datos de carácter personal y están regulados por el artículo 22 LOPD-GDD.

i) *Categorías especiales de datos:* Finalmente, existe un régimen especial reforzado de garantías atribuido a ciertas categorías especiales de datos (anteriormente conocidos como "datos sensibles"), relativos al origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física (artículo 9.1 RGPD). Con carácter general queda prohibido el tratamiento de estos datos, salvo que concurra alguna de las excepciones legalmente establecidas, como, entre otras, el consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados (artículo 9.2 RGPD).

4.3.1.3 Reconocimiento del derecho a la protección de datos personales en la normativa ecuatoriana

La Constitución de 2008 es la primera que reconoce el derecho a la protección de datos personales en Ecuador, lo hace desde el enfoque europeo, con la voluntad de cumplir un alto estándar de protección. El mencionado numeral 19 del artículo 66 de la CRE describe perfectamente uno de los contenidos esenciales del derecho, el relativo a la autodeterminación informativa. No solo prescribe el *acceso* a los datos, como constaba en su antecedente inmediato, el *habeas data*, tanto en la Constitución de 1978, codificada en 1996 como en la Constitución de 1998, sino la *decisión* sobre su información.

En consecuencia, el objetivo fundamental del derecho a la protección de datos personales en Ecuador es el de proteger la autodeterminación informativa de la persona, mediante la implementación y cumplimiento de varios principios propios como: consentimiento informado, calidad, seguridad, finalidad, entre otros; y del ejercicio efectivo de las siguientes garantías: acceso, rectificación, anulación y eliminación. En la configuración de este derecho en la Constitución de 2008 no existe confusión con el derecho a la intimidad o a la privacidad, y en consecuencia se protege todo tipo de datos personales y se supera la determinación histórica, dependiente y atada al derecho a la intimidad que protegía únicamente el dato íntimo, privado, reservado, personal, familiar o sensible, como consta

[301] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Guía de Videovigilancia", 4.

equivocadamente en la normativa legal,[302] pues los datos inocuos o irrelevantes también gozan del estatus de protección, toda vez que cualquiera de estos dependiendo de los tratamientos, procesamientos o formas de difusión pueden potencialmente afectar el libre desarrollo de la personalidad de un individuo y el ejercicio de otros derechos fundamentales.

La doctrina, normativa y jurisprudencia internacional puede tener una configuración generalmente aceptada de un concepto. No obstante, cada país puede establecer sus propias formas de comprensión de una institución o de la naturaleza jurídica de un presupuesto de derecho como es el caso de los datos e información de carácter personal. Es menester analizar los elementos comunes entre esta visión generalmente aceptada y las especificidades de nuestra normativa y verificar si estas pueden ser efectivas de tal forma que no necesiten interpretaciones o reformas, o por el contrario es necesario intervenir ya sea mediante propuestas normativas o reglamentarias que aclaren dudas, eviten confusiones y, en suma, permitan materializar este derecho fundamental.

Este trabajo se enfocará en definir la naturaleza jurídica del dato o información de carácter personal en Ecuador desde la normativa constitucional y de la jurisprudencia existente (*obiter dicta*), ya que hasta la fecha no se ha dictado una ley específica. Pues, solo por medio de una adecuada delimitación se puede determinar los ámbitos de protección y exclusión de este derecho fundamental. Toda vez que no todos los datos ameritan un sistema de protección especializado, sino únicamente los personales, pues permite salvaguardar al individuo desde distintas perspectivas: derechos, intimidad, privacidad, libre desarrollo de la personalidad, autodeterminación informativa e incluso en el ejercicio de otros derechos fundamentales. Además, verificar la procedencia de la garantía constitucional del *habeas data* que viabilice su ejercicio.

4.3.1.4 Naturaleza jurídica del dato personal en la normativa ecuatoriana

En el análisis de los elementos que conforman el concepto de dato personal en la normativa ecuatoriana es menester revisar si en la normativa o en la jurisprudencia se recogen aquellos criterios que han sido desarrollados por la normativa y jurisprudencia internacional.

Al respecto, corresponde analizar el derecho fundamental a la protección de datos personales que consta en el artículo 66, numeral 19, de la CRE que formula: "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley". De tal forma, se deben estudiar los siguientes elementos:

a) *Datos e información:* De la simple lectura del artículo se colige que se usan los términos *datos e información* como sinónimos. Tanto en la normativa como en la jurisprudencia internacional no suele utilizarse el término información, sino únicamente el vocablo *dato* por considerar que de cualquier tipo de dato puede extraerse información y que este término general es suficientemente amplio para incluir en él cualquier: a) soporte: físico o virtual; b) tipo de manifestación: gráfica,

[302] LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS, publicada en el Registro Oficial 557-S, 17-IV-2002, artículo 9: "la recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley".

acústica o fotográfica; c) pauta de expresión: numérica o alfabética; y en general, d) por la diversidad y asociación de la fuente al individuo: como ha ocurrido en otros países donde, paulatinamente, se ha reconocido la condición de dato personal a las direcciones IP, los clics de un usuario, el *log in* a un sitio web, datos biométricos, entre otras.

Sin embargo, respecto de las diferencias entre dato e información la sentencia No. 001-14-PO-CC, de 3 de julio de 2014, dictada por la Corte Constitucional ecuatoriana en su parte argumentativa, que no genera una regla de aplicación obligatoria sino que marca un criterio referencial para orientar la interpretación judicial, señala:

> Sin embargo, se ha identificado en la doctrina sobre la protección de datos una distinción entre los conceptos «dato» e «información» a la que se adscribe esta Corte, como lo relata Osvaldo Gonzaíni: Algunos entienden «datos«» a la representación de hechos, conceptos o instrucciones bajo una forma adaptada a la comunicación, a la interpretación o al tratamiento por seres humanos o máquinas, y por «informaciones» al significado que toman los datos de acuerdo con convenciones vinculadas a éstos. De acuerdo con la distinción conceptual citada, el dato adquiere la calidad de información en tanto cumple una función en el proceso comunicativo.[303]

En la jurisprudencia ecuatoriana, la diferenciación entre dato e información no alude al soporte, al tipo de manifestación, a la pauta de expresión o a la diversidad de la fuente, sino que se refiere a su funcionalidad como medio para establecer una evaluación, apreciación o simbolización del dato, que lo caracteriza como información. La mencionada sentencia alude a esta diferenciación:

> La información, entonces, requiere una interpretación del dato, que dota de carga valorativa y funcionalidad concreta a la descripción que éste hace. Por lo tanto, el dato solamente es relevante para la protección por medio del hábeas data, en la medida en que sea susceptible de cumplir una función informativa. El mismo autor explica dicho proceso de la siguiente manera: El dato es difícil que, por sí solo, pueda tener una incidencia grande o grave en la llamada privacidad. Esto es, mientras el dato no resuelva una consulta determinada, no sirva a un fin, no dé respuestas o no oriente la posible solución a un problema, es el antecedente o punto de partida para la investigación de la verdad; pero, en el momento en que ese mismo dato da respuesta a una consulta determinada, o sirve a un fin, o se utiliza para orientar la solución de un problema, se ha convertido en información. Como conclusión, los datos están protegidos por medio de la garantía constitucional del hábeas data, siempre que cumplan con una función informativa respecto de las personas y sus bienes y por ende, su comunicación, interpretación o tratamiento afecta en mayor o menor medida los derechos de aquel a quien se refieren.[304]

La sentencia transcrita concluye que para los jueces constitucionales ecuatorianos el dato en sí mismo no es objeto de la acción de *habeas data*, sino únicamente aquel que puede llegar a cumplir una finalidad informativa y que en efecto se convierte en información. Esta aseveración debe ser adecuadamente contextualizada porque no puede significar que el derecho a la protección de datos se vea limitado o restringido a proteger únicamente información personal, pues, para que el régimen de protección sea completo, el numeral 19 del artículo 66 de la CRE invoca expresamente los dos

[303] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 001-2014-PJO-CC], ROS No. 281, (3 de julio de 2014).
[304] Ibíd.

términos, tanto *dato* como *información*. Toda vez que, el derecho a la protección de datos personales salvaguarda también los datos personales por sí mismos, en la medida de que aunque aparentemente irrelevantes y carentes de contenido informativo, pueden o tienen el potencial de ser sometidos a un proceso o tratamiento que proporcione un perfil completo de un individuo. Precisamente, por este motivo es que es indispensable implementar mecanismos preventivos como registro de la existencia de bases de datos, sus finalidades y cesiones; así como, controles de verificación a los responsables de ficheros respecto del cumplimiento de los principios como calidad, consentimiento informado, seguridad de la información, entre otros, por parte de entidades especializadas. Es decir, el derecho a la protección de datos personales también tiene como objetivo prevenir o salvaguardar posibles tratamientos que pudieran generar un daño.

La posición jurisprudencial de que el *habeas data* límite su protección a los datos informativos o con función informativa puede provenir de que esta garantía jurisdiccional protege otros derechos como: el honor, el buen nombre, la intimidad personal y familiar.[305] En este sentido, para la transgresión de estos derechos evidentemente se necesita de un dato que genere una evaluación o valoración en un contexto social, familiar o íntimo que cause un daño a la persona. Sin embargo, el *habeas data* también es garantía del derecho a la protección de datos personales, por lo que debe adaptarse al contenido esencial del derecho que tutela; por eso, también se incluye en su ámbito de protección al dato por sí solo, aunque inicialmente carezca de la característica informativa, porque incluso aquel dato que en apariencia no afecta a la privacidad, al decir de la citada sentencia, una vez tratado por medios automatizados puede en conjunto otorgar una visión integral de un individuo que no solo afecten su privacidad e intimidad, sino incidir directamente en el ejercicio de otros derechos fundamentales. En suma, la conclusión que consta en esta sentencia, y que para la jurisprudencia se reconoce como *obiter dicta*, debe utilizarse como mecanismo orientador únicamente en aquellos contextos que le son aplicables.

b) *Datos de carácter personal:* La norma deja expresa constancia de la condición de que el dato debe estar vinculado a un titular para ser considerado de carácter personal. La norma constitucional no hace alusión a si esta forma de asociación entre el dato y el individuo es directa o indirecta, por lo que los elementos de identificado e identificable no han sido desarrollados en la versión ecuatoriana, aunque es común en la mayoría de los ordenamientos jurídicos que esta aclaración conste a nivel legal y no en la norma suprema. Solamente menciona, de manera genérica, que se protegen tanto los datos como la información con la condición de que sean personales. Esta norma, al haberse redactado de forma abierta y general, establece un sistema de protección del derecho a la autodeterminación informativa cualquiera que sea la clasificación del dato: nominativos, innominativos; reservados, secretos o públicos, notorios; sensibles o no sensibles; existenciales o no existenciales;[306] que conste en ficheros de acceso público o en ficheros de naturaleza privada, con la condición *sine quanon*, de que sean personales, esto es asociados a un titular.

[305] TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0070-2003-HD].
[306] O. A. GOZAÍNI, *Hábeas data: protección de datos personales: doctrina y jurisprudencia* (Buenos Aires: Rubinzal-Culzoni Editores, 2001).

4.3.1.5 Análisis de los términos documentos, datos genéticos, bancos o archivos de datos personales e informes en la garantía constitucional de *habeas data*

En Ecuador, la garantía constitucional con la que se permite el ejercicio de los denominados derechos ARCO es el *habeas data* contenido en el artículo 92 de la CRE que señala expresamente que: "Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico [...]".

Al respecto, es necesario analizar cada uno de los términos empleados en este artículo: *documentos, datos genéticos, bancos o archivos de datos personales e informes,* porque lejos de ser abarcadores e incluir todas las formas de manifestación de un dato, que puedan garantizar una protección adecuada del derecho, pueden llegar a restringir su procedencia y a causar confusión.

Sobre este tema, la sentencia No. 001-14-PO-CC, de 3 de julio de 2014, dictada por la Corte Constitucional ecuatoriana, anteriormente estudiada, en su análisis señala:

> 38. El problema respecto de la diferenciación entre conceptos como "documento", "archivo", "dato", "banco de datos", "información" y otros relacionados con la materia, sin duda no es estrictamente jurídico, sino que corresponde también, entre otros campos, al de la informática. Empero, las implicaciones del sentido y alcance que se dé a cada uno de los conceptos enunciados, así como a la correcta diferenciación entre ellos, deberá ser determinado a través de un ejercicio hermenéutico, y por tanto, tendrá directa relación con el contenido del derecho constitucional protegido por medio de la acción de hábeas data. Así, para la solución del caso concreto y la emisión de reglas jurisprudenciales que se deriven de los hechos presentados, esta Corte deberá recurrir a las fuentes doctrinarias que permitan comprender qué protege la garantía jurisdiccional en particular.[307]

La Corte Constitucional señala que es necesario analizar cada caso concreto que se presente y en el que se invoque cada uno de los elementos enlistados en la norma, por el sentido y alcance de cada uno de estos conceptos y sus posibles consecuencias. Además, para un adecuado análisis se deberá acudir a las fuentes doctrinarias;[308] en este sentido a continuación se contribuye con lo siguiente:

a) Documento: La norma por expresa mención regula tanto documentos electrónicos como documentos físicos. Se entiende como *documento físico* "todo escrito legible o descifrable directamente por el ser humano y aportado normalmente en papel (o en el elemento que en cada momento histórico estaba vigente)".[309]

En cambio, el *documento electrónico* es "un instrumento que se confecciona por medio de elementos electrónicos y que solo puede ser leído, comunicado o transmitido con la ayuda de ciertos medios técnicos que hacen perceptibles o inteligibles las señales digitales que lo integran".[310]

---

[307] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 001-2014-PJO-CC].
[308] Ibíd.
[309] J. A. VEGA VEGA, *Derecho mercantil electrónico* (Madrid: Editorial Reus, 2015), 27. ‹http://public.eblib.com/choice/publicfullrecord.aspx?p=4569794›. Consulta: 6 de enero de 2017.
[310] Ibíd.

La diferencia entre este tipo de documentos radica en el soporte, los primeros pueden ser extendidos directamente por el ser humano o a través de ciertos medios técnicos. No obstante, respecto de sus funciones y efectos jurídicos los documentos electrónicos y documentos físicos son equiparables por aplicarse en ellos el principio de equivalencia funcional establecido en el artículo 2 de la Ley No. 67, Ley de Comercio Electrónico, firmas y mensajes de datos del Ecuador, publicado en el Registro Oficial Suplemento 557, de 17 de abril de 2002.

Por cuanto, cada una de las formas de protección que establece el citado artículo puede constar en soporte material o electrónico, es indispensable aclarar que el derecho a la protección de datos resguarda no solo datos virtuales, sino también los físicos, porque se protege el dato personal que ha sido informatizado y también aquel que es susceptible de informatizarse, como por ejemplo: un archivo o fichero con datos no tratados o incluso un fichero físico. Esta informatización se puede llevar a cabo incluso de forma material con la simple "organización y estructura lógica de los datos en un fichero —aunque sea manual—, que permita su fácil acceso, tratamiento y recuperación o consulta de la información".[311]

Respecto de este tema, la sentencia No. 001-14-PO-CC, de 3 de julio de 2014, dictada por la Corte Constitucional ecuatoriana, analizada previamente, en su parte considerativa determina:

> 40. Hechas las distinciones anteriores, cabe señalar que tanto los datos como la información, son conceptos que giran en torno a la capacidad cognitiva atribuida en primera instancia al ser humano, así como a las máquinas como instrumento ordenado a la utilidad que el primero les dé. Al ser tales, entonces, su expresión física por medio de determinadas señales dibujadas sobre un papel, o impulsos eléctricos, variaciones en las ondas, etc., denotan únicamente el medio por el cual se expresan, pero no pueden ser identificados con ellos. Así, si el dato es una representación de determinado fenómeno y la información es el significado de dicha representación adecuada a determinado fin en el proceso comunicativo, el "documento" funge como uno de varios medios en los que es posible impregnar o "imprimir" tal representación por medio de símbolos, a fin de lograr la preservación del dato y la información que se puede extraer de él. Por ende, no interesa para el hábeas data, como garantía, el papel y la tinta utilizados para registrar el dato, ni el disco duro en el cual se encuentre la información -denominados por el constituyente como "soporte material o electrónico" de los datos-, ni cualquier forma ideada por el ingenio humano para su preservación, sino que, como la expresión lo señala, el derecho tutelado recae sobre el dato mismo y el uso informativo que se le dé.[312]

Nuevamente, se analiza la naturaleza del dato y de la información, para concluir que no es importante la forma en la que el dato se presente, sea este físico: imprimible o documentable o virtual: registrado en soporte digital, sino que se protege el contenido informativo. En este sentido, la sentencia realiza un análisis valedero, pues en este caso señala que el *habeas data* no excluye ninguno de los antecedentes de protección, esto es, dato o información en soporte digital o físico.

[311] M. Á. DAVARA RODRÍGUEZ, *Manual de derecho informático* (Navarra: Thomson Aranzadi, Cizur Menor, 2015), 50.
[312] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 001-2014-PJO-CC],.

Ahora bien, superada la discusión sobre la virtualidad o materialidad del dato o la información, el término documento ha propiciado una confusión en el foro ecuatoriano. Ya que se presentan acciones constitucionales de *habeas data* cuando en realidad se pretenden iniciar, ya sea como prueba o diligencia previa, procedimientos ordinarios[313] de mera legalidad, como el de exhibición de documentos.[314]

La Corte Constitucional, en sentencia No. 0044-2007, intenta solucionar esa confusión estableciendo que:

> [...] la diferencia fundamental entre la exhibición de documentos y la acción de habeas data está dada por el tipo de información requerida y la finalidad perseguida con tal acción; para ello, debe tomarse en cuenta que no se trata de cualquier tipo de información sino aquella relacionada con información personal cuya divulgación cause perjuicio o viole su derecho a la intimidad, al honor y a la buena reputación, y que la finalidad es justamente conocer que uso se está dando a esa información, para hacer efectiva la protección de sus derechos.[315]

En tal sentido, la acción de *habeas data*, a diferencia del procedimiento de exhibición de documentos, tiene por finalidad el acceso a los datos para ejercitar el derecho a la autodeterminación informativa o para la implementación de los derechos de rectificación, cancelación y anulación, cuando los datos sean incorrectos, incompletos o desactualizados, todo ello con miras a evitar actos discriminatorios o perjuicios relacionados con la transgresión de otros derechos fundamentales como el honor, la intimidad y ahora la protección de datos personales.

La sentencia No. 001-14-PO-CC, de 3 de julio de 2014, dictada por la Corte Constitucional ecuatoriana, señala como regla de cumplimiento obligatorio por constituir precedente jurisprudencial el siguiente.

> 6. El hábeas data, como mecanismo de garantía del derecho a la protección de datos personales, no podrá ser incoado como medio para requerir la entrega física del soporte material o electrónico de los documentos en los que se alegue está contenida la información personal del titular sino para conocer su existencia, tener acceso a él y

[313] ASAMBLEA NACIONAL DEL ECUADOR, [Código Orgánico General de Procesos, en ROS, No. 506 (22 de mayo de 2015)], *Asamblea Nacional del Ecuador*. ‹http://www.asambleanacional.gob.ec/es/leyes-aprobadas›. Consulta: 18 de febrero de 2018: "Artículo 122.- Diligencias preparatorias. Además de otras de la misma naturaleza, podrá solicitarse como diligencias preparatorias: 1. La exhibición de la cosa mueble que se pretende reivindicar o sobre la que se practicará secuestro o embargo; la del testamento, cuando la o el peticionario se considere la o el heredero, legataria o legatario o albacea; la de los libros de comercio cuando corresponda y demás documentos pertenecientes al comerciante individual, la sociedad, comunidad o asociación; exhibición de los documentos necesarios para la rendición de cuentas por quien se halle legalmente obligado a rendirlas; y en general, la exhibición de documentos en los casos previstos en este Código. 2. La exhibición de los títulos u otros instrumentos referentes a la cosa vendida, por parte de su enajenante en caso de evicción o pretensiones similares. 3. El reconocimiento de un documento privado. 4. El nombramiento de tutora o tutor o curadora o curador para las o los incapaces que carezcan de guardadora o guardador o en los casos de herencia yacente, bienes de la persona ausente y de la o del deudor que se oculta. 5. La apertura de cajas o casilleros de seguridad en las instituciones del sistema financiero. 6. La inspección preparatoria si la cosa puede alterarse o perderse. 7. La recepción de las declaraciones urgentes de las personas que, por su avanzada edad o grave enfermedad se tema fundadamente puedan fallecer o de quienes estén próximos a ausentarse del país en forma permanente o por un largo período".

[314] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0039-2008-HD], ROEE No. 86, (5 de diciembre de 2008.

[315] Ibíd., Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0044-2007-HD], ROS No. 137, (4 de agosto de 2009).

> ejercer los actos previstos en el artículo 92 de la Constitución de la República; el juez está obligado a utilizar todos los mecanismos que establece la ley para efectos de garantizar debida y eficazmente los actos constantes en el artículo referido.[316]

Esta jurisprudencia resuelve una incomprensión, pues clarifica que no se puede usar la acción de *habeas data* para conseguir la entrega física del documento que contiene datos o información personal, sea que este se encuentre en soporte material o electrónico.

Finalmente, Davara en su texto señala que cuando "el dato, o la documentación –como conjunto de datos– son sometidos a un tratamiento o adecuación a un fin, para obtener un resultado elaborado, se convierten en información".[317] Conforme al autor, existe una interpretación por la cual se puede entender al término *documento* como el *conjunto de datos*, de tal forma que no se asocie este término al soporte en el que se encuentren los datos. Esta perspectiva podría solucionar la equivocada compresión que el término documento ha tenido en nuestro país. Ante la imprecisión normativa, es a la Corte Constitucional a la que le corresponde aclarar el sentido en el que debe entenderse el término *documento* para evitar la confusión antes señalada. Además, la alusión a *documento físico o electrónico* en realidad se refiere al soporte en el cual se encontrarán los datos personales, por lo que dicha referencia podría ser suprimida y en la norma únicamente debería constar de forma genérica que se protege el acceso a *datos personales físicos o virtuales* y eliminar el término *documento*.

b) *Dato genético:* El segundo término utilizado es *dato genético*, que como vimos en líneas anteriores se refiere no a las muestras en sí mismas, ya que no pueden ser consideradas datos sino solo fuente de datos,[318] sino a los análisis genéticos, mapas o a los informes o conclusiones que se realicen de la comprensión de dichos resultados. Al parecer su incorporación en el texto constitucional se debe a las dudas, en varios ordenamientos jurídicos extranjeros, sobre su condición de dato personal; de tal forma que los asambleístas ecuatorianos consideraron que era indispensable su expresa mención para evitar estas discusiones o debates y garantizar una protección integral de los datos personales. Anotándose que, sobre este tema conforme ha señalado la autora ecuatoriana María Paulina Casares, una posible solución al tema planteado pasa por la asociación o disociación del dato genético, ya que esta característica de suma importancia definiría el trato que se debe dar a la información genética con el fin de garantizar su confidencialidad.[319]

c) *Bancos o archivos de datos personales o de sus bienes*: La tercera frase utilizada es *bancos o archivos de datos personales o de sus bienes*. Al respecto la cualificación de que estos datos deban pertenecer a bancos o archivos resulta además de innecesaria, impertinente. Ya que, establece una condición excluyente pues solo podría solicitarse *habeas data* respecto de aquellos datos que se encuentren almacenados en un banco o archivo, cuando pueden existir datos sueltos, pero evidentemente relacionados con una persona y que por lo tanto, sean dignos de protección.

---

[316] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 001-14-PO-CC].
[317] M. A. DAVARA RODRÍGUEZ, *Manual de derecho informático*, 53.
[318] J. APARICIO SALOM, *Estudio sobre la protección de datos*, 108.
[319] M. P. CASARES SUBÍA, *La protección de datos genéticos y su impacto en los derecho humanos.* (Ecuador: Observatorio Iberoamericano de Protección de Datos, 2015)

Se ha pronunciado en este sentido el G29 en el Dictamen 4/2007 sobre el concepto de datos personales cuando dice: "para que la información sea considerada como datos personales no es necesario que esté recogida en una base de datos o en un fichero estructurado. También la información contenida en un texto libre, en un documento electrónico puede calificarse como datos personales, siempre que se cumplan los otros criterios de definición de datos personales...".[320] Nuevamente, no es importante la forma de presentación, organización o sistematización del dato o de la información, sino su condición de estar vinculada a una persona.

d) *Informes sobre sí misma, o sobre sus bienes:* Finalmente, la última frase utilizada se refiere a *informes sobre sí misma, o sobre sus bienes.* Cabe analizar en primer lugar lo que se entiende como informe, al respecto la Real Academia de la Lengua en las dos acepciones más cercana al tema de análisis señala que informe es en primer lugar la "Descripción, oral o escrita, de las características y circunstancias de un suceso o asunto" [321]; asimismo dice que es la "Exposición total que hace el letrado o el fiscal ante el tribunal que ha de fallar el proceso"[322].

   En cualquiera de sus dos significaciones el uso del término informe a efectos de establecer la procedencia del *habeas data* hace referencia nuevamente al soporte el que estarán contenidos datos personales sea este oral o escrito. Anotándose que, respecto de la segunda de sus acepciones las exposiciones realizadas en tribunal en el Ecuador constarán grabadas, video grabadas o por escrito, es decir en soporte físico o virtual dependiendo del grado de incorporación de las TIC en cada tribunal o unidad judicial. Se trata del formato en el que se encontrará el dato, pues en esta ocasión estará descrito o será expuesto a través de un informe que puede constar en formato físico o si se trata de un texto, sonido, imagen, fotografía, gráfico, entre otros, puede constar en formato electrónico.

   Nuevamente, resulta equívoco el uso del término *informe* ya que no se deben proteger los datos por constar en un determinado formato sino por su naturaleza en sí misma.

e) *Respecto de la expresión "sobre sí misma o sobre sus bienes":* Al respecto, el G29 en Dictamen 4/2007 determina que:

> […] podría afirmarse que para considerar que los datos versan «sobre» una persona debe haber un elemento «contenido» o un «elemento finalidad» o un elemento «resultado». El elemento contenido está presente en aquellos casos en que de acuerdo con lo que una sociedad suele general y vulgarmente entender por la palabra «sobre» –se proporciona información sobre una persona concreta, independientemente de cualquier propósito que pueda abrigar el responsable del tratamiento de los datos o un tercero, o de la repercusión de esa información en el interesado. La información versa «sobre» una persona cuando se «refiere» a esa persona, lo que debe ser evaluado teniendo en cuenta todas las circunstancias que rodean el caso [...] Se puede considerar que ese elemento finalidad existe cuando lo datos se utilizan o es probable que se utilicen, teniendo en cuenta todas las circunstancias que rodean el caso concreto, con la finalidad de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona.

[320] G29, "Dictamen 4/2007 Sobre el concepto de datos personales".
[321] R. ASALE, "Diccionario de la lengua española - Edición del Tricentenario", *Diccionario de la lengua español*. ‹http://dle.rae.es/?id=LYB2BS5|LYF57Ax›. Consulta: 18 de enero de 2017.
[322] Ibíd.

> Estamos ante una tercera categoría de «sobre» cuando existe un elemento «resultado» [...] porque, teniendo en cuenta todas las circunstancias que rodean el caso concreto, es probable que su uso repercuta en los derechos y los intereses de determinada persona [...].[323]

En ese sentido se ha pronunciado la Corte Constitucional ecuatoriana mediante sentencia en la cual señala expresamente: "la esencia del recurso de hábeas data la información requerida sobre sí mismos, por lo que mediante esta acción no puede ser solicitada información sobre terceras personas sino solo sobre los accionantes, aunque con ello no se persigan causar daño, afectar el honor y en general utilizar dicha información con fines maliciosos".[324] De lo visto, la referencia constitucional del *habeas data* a informes *sobre sí misma* hacen alusión directa a aquellos datos que, ya sea por contenido, finalidad o resultado, están asociados a determinada persona.

Aún más, esta condición se verifica en la expresa mención que realiza la citada norma sobre la frase *informes sobre sus bienes*, ya que precisamente se entiende que "en general, cuando una información versa «sobre» alguien es porque se refiere a ella. Pero no siempre podemos identificar concretamente a la persona. A veces, los datos se refieren a objetos, que pertenecen o están bajo la influencia de alguien, o a procesos o hechos, como por ejemplo el funcionamiento de una máquina cuando requiere intervención humana".[325] Y en este caso, la norma constitucional señala específicamente que el *habeas data* procede respecto de aquellos datos por los cuales una persona, por ser titular de un derecho real, tiene vinculación directa con un bien.

f) Sobre datos sensibles: Si bien, en la normativa internacional no se suele desarrollar un concepto de dato sensible, podemos encontrar las condiciones de su protección en el artículo 92 de la CRE cuando dice: "En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias".

Para identificar la definición de dato sensible, es necesario acudir a la normativa legal. La Ley Orgánica de Transparencia y Acceso a la Información Publica[326] establece una de las condiciones más importantes de los datos sensibles, esto es la confidencialidad; además, determina que existe información personal que está en ficheros estatales y para los cuales no es posible la publicidad, sino por el contrario la reserva, de conformidad con el siguiente texto:

> Artículo 6.- Información Confidencial.- Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República.[327]

Por su parte, la Ley 0, Ley del Sistema Nacional de Registro de Datos Públicos,

[323] G29, "Dictamen 4/2007 Sobre el concepto de datos personales",.
[324] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0023-2008-HD].
[325] I. DAVARA FERNÁNDEZ DE MARCOS, *Hacia la estandarización de la protección de datos personales*, 142.
[326] CONGRESO NACIONAL DEL ECUADOR, [Ley Orgánica de Transparencia y acceso a la Información Pública, Ley 24, en ROS, No. 337 (18 de mayo de 2004)], *Lexis Ecuador*. ‹www.silec.com.ec.› Consulta: 22 de noviembre de 2017).
[327] *Ibíd.*

también señala el concepto de datos sensibles.[328]

Mientras tanto, el artículo 21 del Reglamento a la Ley de Comercio Electrónico, al referirse a la seguridad en la prestación de servicios electrónicos, por los cuales se envía información personal, confidencial o privada, considera datos sensibles del consumidor "sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten".[329] En otras palabras, se considera dato sensible y por tanto amerita mayores niveles de protección aquellos datos que por su naturaleza pueden causar un riesgo en el patrimonio de sus titulares.

Respecto de datos reservados y con carácter de sensibles, el Código de la Niñez y Adolescencia sobre reserva de la información establece:

> Artículo 54.- Derecho a la reserva de la información sobre antecedentes penales.- Los adolescentes que hayan sido investigados, sometidos a proceso, privados de su libertad o a quienes se haya aplicado una medida socio-educativa, con motivo de una infracción penal, tienen derecho a que no se hagan públicos sus antecedentes policiales o judiciales y a que se respete la reserva de la información procesal en la forma dispuesta en esta Ley, a menos que el Juez competente lo autorice en resolución motivada, en la que se expongan con claridad y precisión las circunstancias que justifican hacer pública la información.[330]

En la Ley de Seguridad Pública y del Estado se establece la prohibición expresa de crear bases de datos sensibles por parte de aquellas entidades encargadas de la seguridad integral del Estado y la sociedad, con la finalidad de evitar persecuciones y transgresiones a los derechos de libertad. El artículo en mención señala:

> Artículo 22.- De la prohibición.- Ningún organismo de inteligencia está facultado para obtener información, producir inteligencia o almacenar datos sobre personas, por el solo hecho de su etnia, orientación sexual, credo religioso, acciones privadas, posición política o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción.[331]

Otra de las normas que desarrolla el concepto de dato sensible consta en la Ley del Sistema Nacional de Registro de Datos Públicos que, pese a su limitado ámbito relativo a instituciones públicas, delegadas o que brindan servicios públicos, establece varios de los derechos, principios y contenidos del derecho a la protección de datos personales. Respecto de los datos sensibles, consta en el artículo 6 de la citada ley una lista de datos que por su naturaleza de ser posible fuente de daño a los derechos

---

[328] ASAMBLEA NACIONAL ECUADOR, [Ley 0, Ley del Sistema Nacional de Registro de Datos Públicos, en ROS, No. 162 (31 de marzo de 2010), Ultima modificación: 12 de septiembre de 2014], *Lexis Ecuador*. ‹www.silec.com.ec›.

[329] PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR, [Reglamento a la Ley de Comercio Electrónico. DEJ 3496, en RO, No. 735 (31 de diciembre de 2002)], *Lexis Ecuador*. ‹www.silec.com.ec›. Consulta: 22 de noviembre de 2017.

[330] CONGRESO NACIONAL DEL ECUADOR, [Código de la Niñez y Adolescencia. Ley 100, en RO, No. 737 (03 de enero de 2003)], *Lexis Ecuador*. ‹www.lexis.com.ec›. Consulta: 2 de junio de 2017.

[331] ASAMBLEA NACIONAL DEL ECUADOR, [Ley de Seguridad Pública y del Estado. Ley 0, en ROS, No. 35 (28 de septiembre de 2009)], *Lexis Ecuador*. ‹www.silec.com.ec›. Consulta: 22 de noviembre de 2017.

fundamentales de sus titulares deben contar con un sistema de protección especial, en este caso la condición de confidencialidad, y además la obligatoriedad de establecer altos niveles de seguridad. Se añade además que, conforme la doctrina y la normativa internacional, esta lista es solamente ejemplificativa y no taxativa. El mencionado artículo dispone lo siguiente:

> Artículo 6.- Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales. El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial. También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado. La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos. Para acceder a la información sobre el patrimonio de las personas el solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará de la misma y consignar sus datos básicos de identidad, tales como: nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el/la titular de la información pueda ejercer. La Directora o Director Nacional de Registro de Datos Públicos definirá los demás datos que integrarán el sistema nacional y el tipo de reserva y accesibilidad.[332]

La Ley del Sistema Nacional de Registro de Datos Públicos[333] establece entre una de sus prioridades la creación de un sistema unificado de datos públicos registrables; es decir, el registro de datos respecto de los bienes o patrimonio de las personas naturales o jurídicas, por parte de las instituciones del sector público y privado que actualmente o en el futuro administren bases o registros de datos públicos. Esta inscripción, respecto de la titularidad de derechos reales asociados a persona o personas determinadas, tendría como finalidad la de plasmar el modo de adquirir el dominio y otros derechos reales de los bienes raíces mediante la denominada *tradición*; de contribuir a dar publicidad de los actos y contratos en garantía de los derechos de terceros; y de garantizar la autenticidad y seguridad de los títulos, instrumentos públicos y documentos.

Anotándose que, si bien el artículo 2, numeral 3, literal d, de la LOPDP española establece que los tratamientos de datos personales derivados de Registro Civil se regirán por sus disposiciones específicas. En el caso ecuatoriano, no se ha dictado una ley de protección de datos personales que excluya a estos ficheros y establezca un sistema especial de protección; por eso, deben protegerse desde la perspectiva del derecho a la protección de datos personales no solo aquellos que constan en esta base de datos, sino aquellos datos que deberán constar inscritos en el registro de la propiedad, en el registro mercantil, y en general en todos aquellos ficheros regentados

[332] Ibíd., [Ley 0, Ley del Sistema Nacional de Registro de Datos Públicos, en ROS, 162 (31 de marzo de 2010), Última modificación: 12 de septiembre de 2014].
[333] Ibíd.

por las instituciones que componen el Sistema Nacional de Registro de Datos Públicos, contemplados en la Ley del Sistema Nacional de Registro de Datos Públicos publicada en Registro Oficial Suplemento No. 162, de 31 de marzo de 2010.

El artículo 6 de la mencionada ley establece que se deberá garantizar niveles de seguridad y confidencialidad de aquellos datos de carácter personal, relativos a ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales. Dicho de otro modo, se reconoce que estas bases tratarán datos personales confidenciales y por tal motivo, las instituciones responsables de los ficheros deberán establecer niveles de seguridad para la protección especial a estos datos sensibles. Asimismo, en el Reglamento a Ley del Sistema Nacional de Registro de Datos Públicos, en la Disposición General Séptima se señala:

> Para los fines del presente Reglamento, se establecen las siguientes definiciones: 3. Datos confidenciales.- Es toda información a la que solo los titulares pueden acceder tales como los datos personales especialmente protegidos que se refieren a: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución de la República e instrumentos internacionales.[334]

Finalmente, el artículo 11 del Reglamento a la Ley del Sistema Nacional de Registro de Datos Públicos dispone desarrollar los principios que deberán aplicarse para el tratamiento de datos personales contenidos en estas bases de datos.

En suma, los datos sensibles en Ecuador tienen un marco de protección sectorial, ya que constan protegidos desde el ámbito de la seguridad nacional, de los ficheros cuyo responsable es el Estado, e incluso desde el ámbito patrimonial y de servicios electrónicos. Sin duda, son iniciativas fundamentales pero que aún no son suficientes pues no abarcan toda la complejidad del sistema de protección, especialmente en el ámbito privado.

g) *Sobre datos e información en el habeas data:* El artículo 92 de la CRE, al describir al *habeas data*, señala expresamente que será procedente respecto de *documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes*. Sin embargo, no existe mención expresa a los términos genéricos *datos e información*, como reza en el artículo 66, numeral 19, de la Constitución, en su lugar se optó por una enunciación innecesaria, imprecisa, contradictoria, que en la práctica no ha permitido un adecuado ejercicio de esta garantía constitucional. De esta manera, incluso la garantía constitucional de *habeas data*, al no mencionar el vocablo *dato*, se encontraría incompleto y sería insuficiente para determinar un adecuado marco de protección porque se debe proteger al presupuesto en sí mismo y no a sus manifestaciones, representaciones, formatos o procesamientos, precisamente para evitar que en el avance de la tecnología existan datos que puedan quedar fuera del

[334] PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR, [Reglamento a Ley del Sistema Nacional de Registro de Datos Públicos en la Disposición General Séptima DEJ 950 - RS 718 - 23/mar/2016], *Lexis Ecuador*. ‹www.silec.com.ec›. Consulta: 22 de noviembre de 2017.

régimen de protección por no calzar en ninguna de las expresiones constantes en la norma. El uso de un término general permite que en la medida en la que se van presentando avances en la materia —léase correo electrónico, nombres de dominio, direcciones IP, entre otras— la norma pueda seguir vigente, y por lo tanto, constituirse en mecanismo real de la vigencia y efectividad de la norma.

h) *Normativa legal y reglamentaria:* Terminado el análisis de la Constitución, resta examinar la normativa legal, en este caso la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial 557-S, 17-IV-2002; esto es con anterioridad a la Constitución del 2008 que reconoce a la protección de datos en el Ecuador como derecho fundamental. En consecuencia, dicho cuerpo legal concibe los datos personales desde una perspectiva limitada a datos íntimos, tal como lo señala la disposición general octava, en el glosario de términos, cuando describe que: "Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley". Más aún existe una mención expresa en el artículo 9 de la ley en cuestión que señala que "la recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley". Por consiguiente, esta norma vigente se encuentra erróneamente anclada a un anterior sistema ya superado, por el cual no se reconocía la existencia del derecho a la protección de datos como derecho autónomo; sin embargo, por imperar en Ecuador el principio de aplicación directa de la Constitución (artículo 11 numeral 3 CRE), se obviará esta ley y se aplicará directamente la norma constitucional en aquellos casos sometidos a conocimiento de autoridades públicas o judiciales.

   Finalmente, no existe normativa que determine si las imágenes recogidas mediante sistemas de videovigilancia pueden ser consideradas datos personales, desde una lectura progresiva del derecho; además, de una interpretación general del concepto de dato personal no importaría el soporte, ni la tipología del dato, si está automatizado, es automatizable o es incluso suelto, sino que puede ser relacionado a persona identificada o identificable.

4.3.1.6 Conclusiones

Conforme consta en el numeral 19 del artículo 66 de la Constitución de la República del Ecuador, el presupuesto del derecho a la protección de datos personales es *el dato y la información de carácter personal*.

La posición jurisprudencial referencial que limita la procedencia del *habeas data* a los datos informativos o con función informativa, debiera ser aplicada solo a los otros derechos protegidos por esta garantía jurisdiccional como: el honor, el buen nombre y la intimidad personal y familiar, en vista de que, en el caso del derecho a la protección de datos personales, el *habeas data* debe adaptarse al contenido de este derecho fundamental y resguardar no solo el dato con contenido informativo, sino también proteger al dato por sí solo, porque, aunque inicialmente carece de la característica informativa, puede ser tratado, perfilar a un individuo y afectar su autodeterminación informativa e incluso otros derechos fundamentales.

Adicionalmente, en el artículo 92 de la CRE no existe mención expresa a los términos genéricos *datos e información*. La garantía constitucional se encontraría incompleta y sería insuficiente para determinar un adecuado marco de protección porque se debe proteger al dato y a la información, y no solo a sus manifestaciones o procesamientos, precisamente para evitar que en el avance de la tecnología existan datos que pudieran quedar fuera del régimen de protección por no calzar alguna de las expresiones constantes en la norma, esto es *documentos, datos genéticos, bancos o archivos de datos personales e informes sobre sí misma, o sobre sus bienes*.

Tanto la norma que hace alusión al derecho fundamental como aquella que consagra la garantía constitucional del *habeas data*, deben proteger el acceso, decisión y gestión del dato o de la información, incluidos de forma expresa los datos genéticos, en cualquier soporte físico virtual, ya sean que estos consten en documentos o informes, se encuentren de forma aislada o incorporados a archivos o bancos de datos, o sean parte o no de cualquiera otra forma de recogida o procesamiento y versen sobre la persona misma o sobre sus bienes. La única condición clara y coincidente es que estos datos deben vincularse a personas identificadas o identificables, no necesariamente íntimos como consta equivocadamente en la normativa legal existente, sino que todo tipo de dato personal incluso aquel considerado inocuo que amerita protección en virtud de su potencialidad y de los actuales avances en minería de datos y la elaboración de perfiles.

4.3.2 Titulares o sujetos activos: primer elemento del contenido esencial

Dentro del contenido esencial del derecho a la protección de datos personales el primer elemento que vamos a analizar se refiere a las personas a las que favorece este derecho fundamental. En este sentido, es necesario realizar una determinación de si los titulares pueden ser personas naturales y personas jurídicas, ya que sobre el tema ha existido mucha controversia que, sin embargo, paulatinamente se va decantando por un reconocimiento de las personas jurídicas como titular de derechos fundamentales, entre ellos la protección de datos personales.

4.3.2.1 Titulares o sujetos activos

Conforme la metodología planteada procede establecer el metalenguaje o ideas generalizadas y convicciones generalmente admitidas entre los juristas, los jueces y, en general, los especialistas en derecho respecto de la titularidad o sujetos activos del derecho a la protección de datos personales.

Tradicionalmente, se ha concebido que solo las personas físicas sean titulares de derechos fundamentales, en virtud de que es obligación de todo poder del Estado respetar y proteger la dignidad humana, conforme aparece en la Ley Fundamental de Bonn. "La dignidad del ser humano y los derechos humanos inviolables e inalienables son la base sobre la que se elevan los derechos fundamentales con las garantías constitucionales".[335] En tal sentido, solo eran titulares las personas naturales puesto que únicamente a ellas les era atribuible en esencia el concepto de dignidad humana. Sin embargo, la propia Ley citada señala, en el numeral 3 del artículo 19, al referirse a la restricción de los derechos afirma que: "Los derechos fundamentales rigen también para las personas jurídicas con sede en el país, en tanto que por su propia naturaleza sean aplicables a las mismas". Por tanto, en Alemania existe una

[335] M. CARRASCO DURÁN Y J. PÉREZ ROYO, *Curso de derecho constitucional*, 191.

declaración expresa, respecto a otorgar la titularidad de ciertos derechos a las personas jurídicas.

Acerca de la normativa constitucional española, no consta expreso reconocimiento a la titularidad de derechos fundamentales de las personas jurídicas, así como tampoco aparece prohibición específica. Es la Corte Constitucional española la que al realizar el análisis del derecho al honor, aclara lo siguiente:

> Nuestra Constitución configura determinados derechos fundamentales para ser ejercidos de forma individual; en cambio otros se consagran en el Texto constitucional a fin de ser ejercidos de forma colectiva. Si el objetivo y función de los derechos fundamentales es la protección del individuo, sea como tal individuo o sea en colectividad, es lógico que las organizaciones que las personas naturales crean para la protección de sus intereses sean titulares de derechos fundamentales, en tanto y en cuanto éstos sirvan para proteger los fines para los que han sido constituidas. En consecuencia, las personas colectivas no actúan, en estos casos, sólo en defensa de un interés legítimo en el sentido del artículo 162.1 b) de la C. E., sino como titulares de un derecho propio".[336]

En consecuencia, para la jurisprudencia española las personas jurídicas tienen la posibilidad de accionar garantías constitucionales, pero no solo se trata de identificarlos como parte procesal con un interés legítimo, sino sobre todo de constituírsele como legítimos contradictores, en la medida en que solo un titular de un derecho puede discutir y favorecerse o no de una sentencia de fondo en la que se verifica sin un derecho le es o no atribuible.

Asimismo, la titularidad de los derechos no es absoluta ya que:

> [...] por falta de una existencia física, las personas jurídicas no pueden ser titulares del derecho a la vida, del derecho a la integridad física, ni portadoras de la dignidad humana. Pero si el derecho a asociarse es un derecho constitucional y si los fines de la persona colectiva están protegidos constitucionalmente por el reconocimiento de la titularidad de aquellos derechos acordes con los mismos, resulta lógico que se les reconozca también constitucionalmente la titularidad de aquellos otros derechos que sean necesarios y complementarios para la consecución de esos fines. [...] En ocasiones, ello sólo será posible si se extiende a las personas colectivas la titularidad de derechos fundamentales que protejan —como decíamos— su propia existencia e identidad, a fin de asegurar el libre desarrollo de su actividad, en la medida en que los derechos fundamentales que cumplan esta función sean atribuibles, por su naturaleza, a las personas jurídicas. Bajo esta perspectiva destaca la STC 23/1989, en la que se afirma que este Tribunal «ha venido considerando aplicable, implícitamente y sin oponer reparo alguno, el artículo 14 C.E. a las personas jurídicas de nacionalidad española, como titulares del derecho que en él se reconoce, como se pone de manifiesto, entre otras, en las SSTC 99/1983, 20 y 26/1985 y 39/1986, sin que existan razones para modificar esta doctrina general»…".[337]

Únicamente, es posible la titularidad de derechos fundamentales de las personas jurídicas en aquellos casos en que los criterios de existencia material y de dignidad no son aplicables, por eso deberá analizarse la naturaleza de cada uno de los derechos fundamentales. Esta titularidad solo procederá en aquellos casos en los cuales ha sido transgredida o existe riesgo de afectación la propia existencia e identidad, que perturbe el libre desarrollo de la actividad, de la persona jurídica.

[336] TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 139/1995].
[337] Ibíd.

En ese contexto, resta identificar si la protección de datos personales es de aquellos derechos fundamentales que requieren de una atribución de dignidad o de necesaria materialidad por parte de su titular. Si la respuesta fuera positiva, no podrían gozar de este derecho las personas jurídicas. Ahora bien, en aquellas sentencias que asociaban la protección de datos personales al derecho a la intimidad, a tal punto de considerarla como una simple manifestación de esta última, se entendía que era imputable solo a personas físicas por la directa relación con el ámbito más personal, propio, íntimo o privado de una persona;[338] es decir, era indispensable un contenido de dignidad, pues solo las personas físicas tienen derecho a la intimidad, lo que eliminaba la titularidad de las personas jurídicas.

No obstante, al visibilizar al derecho a la protección de datos como autónomo e independiente, y en consecuencia no asociado a la intimidad porque protege bienes jurídicos distintos como la autodeterminación informativa, la libertad informática, los derechos ARCO y varios principios específicos y en contextos en que como derecho instrumental consolida "no solo la protección de los ciudadanos frente al uso inadecuado de técnicas informáticas, sino, en un sentido más extenso, la protección de cualesquiera derechos fundamentales y libertades públicas de las personas frente al tratamiento automatizado de sus datos de carácter personal",[339] se vuelve posible que personas jurídicas puedan ser titulares, en la medida en que no es de la naturaleza del derecho que solo se produzca la transgresión en la materialidad de una persona, ni tampoco el bien jurídico se refiere a una cualidad exclusiva de la dignidad humana. Por el contrario, es absolutamente posible la transgresión de datos personales de personas jurídicas en ciertos casos específicos y que pueden llegar a afectar su desarrollo en sociedad.

Similar razonamiento encontramos en la Memoria 2001 de la AEPD que, además de distinguir el derecho a la protección de datos del derecho a la intimidad, considera que aquellos empresarios individuales en el ejercicio de sus actuaciones comerciales podrían ser sujetos de tutela del derecho a la protección de datos personales, ya que mediante la vulneración de los datos de una persona se pueden llegar a transgredir otros derechos fundamentales, como se señala a continuación: "Ello supone que, si bien los empresarios individuales pueden carecer de un derecho a la intimidad personal y familiar, ello no implica que el tratamiento de los datos referidos a los mismos pueda dar lugar a una vulneración de otros derechos que les atribuye la Constitución (por ejemplo, el tratamiento de los datos relacionados con la pertenencia de un empresario a una determinada asociación puede vulnerar el derecho de asociación, consagrado por el artículo 22 de la Constitución...".[340]

Si bien, la LOPD[341] española no reconoce protección a las personas jurídicas; sin embargo, la propia Corte Constitucional española, e incluso la Agencia Española de Protección de Datos, como se analizó en líneas anteriores, reflexiona que respecto de los posibles titulares entre

[338] J. APARICIO SALOM, *Estudio sobre la protección de datos*, 92-95.

[339] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Memoria 2001". ‹http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2001/MEMORIA_2001.pdf›. Consulta: 21 de enero de 2017.

[340] Ibíd.

[341] España, *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*: "Artículo 1. Objeto. La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. [...] Artículo 3. Definiciones. A los efectos de la presente Ley Orgánica se entenderá por: [...] e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo". Diciembre 13, 1999, BOE núm. 298, de 14 de diciembre de 1999, págs. 43088 a 43099 (12 págs.).

ellos, personas jurídicas, debería atenderse "en cada caso concreto a una adecuada protección de los derechos fundamentales consagrados en la Constitución".[342] Ya que, en ciertos casos, podrían afectarse derechos fundamentales mediante transgresiones a sus datos; precisamente, aquello que configura la necesidad de reconocerle este derecho a estos entes ficticios.

Por su lado, la comunidad europea permitió que cada Estado resuelva el tema. El Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la *Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, en el artículo 3, literal b, establecía la posibilidad de que en lo relativo al campo de aplicación: "Cualquier Estado podrá —en el momento de la firma o al depositar su instrumento de ratificación, aceptación, aprobación o adhesión, o en cualquier otro momento ulterior— hacer saber mediante declaración dirigida al servicio general del Consejo de Europa [...] b) Que aplicará el presente Convenio, asimismo, a informaciones relativas a agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica".[343] En consecuencia, cada país podía optar por incluir o no en su normativa interna la protección de los datos para colectivos o para personas jurídicas.

España no hizo uso de esa posibilidad, conforme consta en el artículo 2 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre. Allí se señala que:

> [...] este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

Esta norma se motiva en la concepción de que las personas jurídicas están reguladas por otras leyes como las de sociedades, patentes, marcas, defensa de la competencia, etc., y en estos ámbitos pueden encontrarse mecanismos de protección para su información. Asimismo, las personas naturales que integran a las personas jurídicas o incluso los profesionales y empresarios individuales cuando sus datos han sido tratados solo en consideración de empresarios, es decir, por pertenecer al ámbito mercantil, no gozan de protección, exceptuándose cuando los datos de su actividad profesional empresarial coinciden con la vida privada del individuo, lo que deberá valorarse caso a caso.

Como vemos no es unívoca la identificación de quienes gozan del derecho a la protección de datos personales, pues dependiendo de los criterios constitucionales o legales adoptados por cada país es posible que se reconozca o no la titularidad a las personas jurídicas, más aún llama la atención los matices o excepciones que pueden presentarse en aquellos países cuya legislación expresamente lo haya dejado por fuera.

4.3.2.2 Titulares o sujetos activos en la normativa ecuatoriana

[342] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Memoria 2001".
[343] CONSEJO DE EUROPA, *Convenio No. 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*.

De conformidad con el artículo 10 de la Carta Magna del Ecuador se concede personalidad jurídica a toda persona, comunidad, pueblo, nacionalidad, colectivo,[344] e incluso se considera a la naturaleza como sujeto de derechos. A cada uno de estos titulares, atendiendo a sus condiciones particulares, se le garantiza derechos con características y contenidos que les permiten su adecuado desarrollo en sociedad.

En ese sentido, el artículo 66 de la CRE recoge los derechos propios de las personas individuales. Asimismo, otorga derechos adecuados y pertinentes para proteger a las personas que integran aquellos colectivos considerados de atención prioritaria y que constan descritos en el capítulo tercero de la Constitución denominado *Derechos de las personas y grupos de atención prioritaria*: Adultas y adultos mayores, Jóvenes, Movilidad humana, Mujeres embarazadas, Niñas, niños y adolescentes, Personas con discapacidad, Personas con enfermedades catastróficas, Personas privadas de libertad y Personas usuarias y consumidoras. Los pueblos, nacionalidades y comunidades gozan de los derechos contenidos en el artículo 57 de la Carta Fundamental; y por su parte, la naturaleza constituye sujeto de aquellos derechos que expresamente se le garantizan en los artículos 71 y 72 de la Constitución.

Se aclara además que al haberse eliminado las clasificaciones tradicionales de derechos civiles, políticos, y económicos, sociales y culturales se eliminaron las distinciones respecto a la aplicación prevalente entre unas y otras, permitiendo que todos estos derechos sean justiciables, con el objetivo de garantizar la efectiva vigencia de los derechos. La Constitución de 2008 al establecer una división temática en: derechos de participación, derechos de libertad, derechos del buen vivir, de las personas y de los grupos de atención prioritaria, entre otros, enfatiza el carácter integral, complementario y la igual jerarquía de todos los derechos constitucionales. Incluso al referirse a los derechos colectivos, la Constitución de 2008 prefiere denominarlos *derechos de las comunidades, pueblos y nacionalidades*, para así destacar que también otros derechos pueden exigirse eventualmente de forma colectiva.[345]

El numeral 7 del artículo 11 de la CRE al establecer los principios que rigen el ejercicio de los derechos fundamentales señala que se puede ser titular no solamente de los derechos atribuidos particularmente a cada titular, sino de todos aquellos derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos

[344] J. CÉSAR TRUJILLO Y R. ÁVILA SANTAMARÍA: "Este enunciado rompe la tradición liberal de considerar que existen derechos individuales y –excepcionalmente– derechos colectivos. Todos los derechos humanos pueden ser ejercidos de forma individual o colectiva. La forma de ejercicio colectivo puede ser variada. La enumeración comienza con las personas, que pueden intervenir de forma individual o como parte de un colectivo. Siguen las comunidades, que pueden abarcar a grupos humanos que no cuadran con los conceptos de pueblo o nacionalidad. Las comunidades podrían tener vínculos geográficos, como la comunidad de Oyacahi, o vínculos de identidad por su opción sexual, como la comunidad GLBT (gay, lesbiana, bisexual y travesti (sic)). Las nacionalidades colectivas formadas a lo largo de la historia y que comparten la misma identidad étnica, cultural, lingüística, etc., como la nación Quichua, Shuar, entre otras. En el Ecuador, los pueblos son subdivisiones de la nacionalidad Quichua que se identifican por algunos rasgos específicos que no comparten con los otros pueblos como el pueblo Cayambi, por ejemplo. Hay además los colectivos, entidades integradas por personas que forman parte de manera temporal de una categoría social a los que –como partes de esa categoría– se les reconoce derechos específicos. Es el caso, por ejemplo, de los niños, niñas, adolescentes y otros a los que Peces Barba denomina 'personas situadas'. Finalmente, hay colectividades conformadas por individuos que tienen el interés común de que les reconozca sus derechos por las mismas razones o fundamentos jurídicos". J. C. TRUJILLO Y R. ÁVILA SANTAMARÍA, "Los Derechos en el Proyecto de Constitución", en *Análisis nueva constitución* (Quito: ILDIS, Friedrich Ebert Stiftung, 2008), 70.
[345] Ibíd., 71.

incluidos aquellos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades, cuando sean pertinentes para su pleno desenvolvimiento en sociedad. De esta forma, se genera un sistema de derechos sistémico, integrado, complementario y progresivo, que por vía normativa intenta ser efectivo.

Coincide con esta postura, lo dispuesto en el numeral 1 del artículo 11 de la Constitución, por el cual todos los derechos, independientemente de sus titulares específicos, pueden ser ejercitados, promovidos o exigidos de forma individual o colectiva. Además, los titulares puedan reclamar cualquier derecho que conste en la Constitución y en los instrumentos internacionales de derechos humanos incluidos aquellos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades; mediante las garantías constitucionales existentes, de conformidad con lo señalado por el artículo 86 de la CRE cuando se indica que cualquier persona, grupo de personas, comunidad, pueblo o nacionalidad podrá proponer las acciones previstas en la Constitución.

Ahora bien, respecto de la titularidad del derecho a la protección de datos personales, materia de esta investigación, desde una aproximación básica, pareciera que solo le es invocable a la persona individual, esto por cuanto de la redacción del numeral 19 del artículo 66 de la Constitución, consta la expresa mención en la parte inicial de la norma citada que los derechos se reconocen y garantizan a las personas. Además, esta norma consta en el título II llamado *Derechos*, en el capítulo sexto denominado *Derechos de Libertad*; en otras palabras, la alusión directa a los derechos de las personas individuales.

Sin embargo, luego del análisis realizado es obvio que los titulares serán no solo las personas individuales, sino también las comunidades, pueblos, nacionalidades o colectivos, desde la perspectiva de que todos ellos son titulares reconocidos en la CRE, artículo 10; que todos los derechos y garantías pueden ser reclamados de forma individual y colectiva, numeral 1 del artículo 11 y numeral 1 del artículo 82 de la Constitución; y finalmente, que todos estos titulares lo son de todos los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos incluidos aquellos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades, numeral 7 del artículo 11 de la Constitución. Dicho de otro modo, que todos estos titulares deben ser respetados y valorados por sí mismos y en su relación con otros, por contener características y condiciones particulares que los individualizan como grupo y que los vuelve únicos y trascendentales; esto es, poseen una dignidad propia y distinta de los individuos que la conforman.

Además, por la naturaleza misma del derecho a la protección de datos personales, deben estar protegidos todos aquellos titulares cuyos datos pudieran ser recolectados, archivados, procesados, distribuidos o difundidos sin su autorización o sin el mandato de la ley; es decir, aquellas acciones que pudieran causarles un perjuicio directo a su dignidad o, por intermedio de ellos, violentar otros derechos fundamentales.

Cabe anotar que existen varios registros, en general de acceso público, regentados por el Estado y dispuestos por leyes específicas que obligan a comunidades, pueblos, nacionalidades y colectividades a registrar datos propios, diferenciados e independientes de quienes los integran, por ejemplo: el Sistema Unificado Información de Organizaciones Sociales.[346]

[346] Ecuador, Reglamento Sistema Unificado Información de Organizaciones Sociales, 2013: "Artículo 7.- Obligaciones de las organizaciones.- Sin perjuicio de las obligaciones establecidas en otras disposiciones normativas, las organizaciones sociales tendrán las siguientes obligaciones: [...] 3. Entregar a la entidad

Queda analizar si los artículos 10 y el inciso inicial del artículo 66 de la CRE, al utilizar el término *persona*, incluyen dentro del concepto tanto a las personas físicas como a personas jurídicas. Si bien, en ninguno de los dos artículos se hace alusión expresa al reconocimiento de los entes morales o las ficciones jurídicas como titulares de derechos. Si existe expresa atribución de personalidad jurídica a entes abstractos que configuran el Estado plurinacional (comunidades, pueblos y nacionalidades), así como a colectivos (mujeres, niños, niñas y adolescentes, adultos mayores, entre otros); por tanto, en Ecuador es posible el reconocimiento como titulares de derechos a entes inmateriales o a un grupo de personas unidas por una identidad u objetivo común.

Para clarificar si las personas jurídicas se incluyen en la utilización de la frase *toda persona*, corresponde el análisis la sentencia vinculante[347] No. 001-14-PO-CC, de 3 de julio de 2014, dictada por la Corte Constitucional, que justamente resuelve esta situación, para lo cual es pertinente, en primer lugar, analizar las consideraciones y fundamentos de la Corte Constitucional que dicen lo siguiente:

> 22. Es claro que los términos en que tal universalidad se expresa y hasta donde esta se extiende dependerá de cada diseño constitucional en particular; sin embargo, dicha noción remite, sin lugar a dudas, a una expansión hermenéutica de los términos, y no a una reducción, debido al concepto de igualdad que demanda que como única condición para que se considere a un sujeto como titular de derechos constitucionales, sea ajustarse al parámetro mínimo que la Constitución presente para su aplicación. En el caso del Ecuador, dicho parámetro se cumple con pertenecer a alguno de los géneros «personas», «comunidades», «pueblos», «nacionalidades», «colectivos». Como se puede advertir de una interpretación literal del texto constitucional, entonces, el término «personas», en tanto se refiere a la titularidad de los derechos constitucionales, no debe excluir a priori a una especie del género, como son las personas jurídicas. 23. Se podrá, sin duda, oponer a la conclusión anterior el que existen derechos constitucionales cuyo ejercicio no puede darse por parte de una persona jurídica, debido a sus características propias, distintas a las de un ente corpóreo, con características biológicas y psicológicas propias de los seres humanos. Un ejemplo, de entre muchos que se podrían presentar en apoyo a tal afirmación, es el derecho a la integridad psíquica reconocido en el artículo 66 numeral 3 literal a de la Constitución de la República. Empero, es criterio de esta Corte que el hecho de que ciertos derechos constitucionales no puedan ser ejercidos por alguno de los sujetos, no constituye una exclusión respecto de su calidad de tales.[348]

Conforme la motivación transcrita se entiende que para el Ecuador, el término *persona* utilizado tanto en el artículo 10, como en el artículo 66 de la CRE sobre el catálogo de los derechos de libertad, cuyo numeral 20 consagra el derecho a la protección de datos personales, se refiere tanto a la persona física como a la persona jurídica.[349] En consecuencia,

---

competente del Estado la documentación e información establecida en este Reglamento en forma completa y clara, incluyendo la que se generare en el futuro como consecuencia de la operatividad de la organización social".

[347] CONSTITUCIÓN REPÚBLICA DEL ECUADOR [2008], artículo 436, numeral 6: "La Corte Constitucional ejercerá, además de las que le confiera la ley, las siguientes atribuciones: [...] 6. Expedir sentencia que constituya jurisprudencia vinculante respecto de las acciones de protección, cumplimiento, hábeas corpus, hábeas data, acceso a la información pública y demás procesos constitucionales, así como los casos seleccionados por la Corte para su revisión".

[348] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 001-2014-PJO-CC].

[349] ASAMBLEA NACIONAL DEL ECUADOR, [Código Civil Codificado, ROS, No. 46 (24 de junio de 2005), Última modificación: 08 de julio de 2019]: "Artículo 564.- Se llama persona jurídica una persona ficticia, capaz de ejercer derechos y contraer obligaciones civiles, y de ser representada judicial y extrajudicialmente".

estos, además de los otros titulares constantes en el artículo 10 de la Constitución: pueblos, nacionalidades, comunidades y colectivos serán titulares de aquellos derechos constitucionales, en los que el criterio de materialidad o de dignidad del titular para el ejercicio del derecho no sea indispensable. Aclarando que, en el caso de pueblos, nacionalidades, comunidades e incluso de los colectivos, estos tienen reconocida una dignidad propia que los caracteriza y distingue de tal forma que logra en sus miembros un elemento unificador y homogeneizador con el cual les asigna unas características y condiciones propias que deben ser garantizadas por el Estado.

Pero además, en la sentencia N.° 068-10-SEP-CC, la Corte Constitucional para el período de transición realiza la siguiente precisión: "En torno a esta apreciación realizada por la parte recurrida, esta Corte reitera que pese a que las personas jurídicas no sean titulares de todos los derechos constitucionales fundamentales, sí lo son de aquellos que les correspondan, según su naturaleza social y siempre en atención a la definición constitucional de los derechos de los que se trate, condición de la cual el Estado en sí no es ajeno y que, además, algunos de los derechos constitucionales fundamentales sólo son predicables de ciertas personas naturales, como es el caso de los derechos constitucionales fundamentales de los niños, el de la no extradición de nacionales y el de los derechos políticos, entre otros; inclusive, en este mismo sentido y bajo las reservas doctrinarias y dogmáticas respectivas, se ha concluido que algunos derechos constitucionales fundamentales no son predicables de todos los individuos en general".[350]

Es menester analizar si el derecho a la protección de datos personales es de aquellos que ya sea por su naturaleza social o las condiciones de materialidad y dignidad de los titulares puede ser ejercido por una persona jurídica. Al respecto, la sentencia citada en las consideraciones y fundamentos de análisis menciona lo siguiente:

> 28. La autodeterminación informativa está supeditada, entonces, a la existencia de información que atañe a determinado sujeto y a la necesidad de que este tenga una esfera mínima de actuación libre respecto de dicha información, sobre la cual no debería existir una interferencia ilegítima por parte de terceros; asimismo, implica la posibilidad de que dentro de los límites que franquean la Constitución y la Ley, se tenga capacidad para ejercer cierto control sobre el uso que se haga de tal información, aunque el poseedor de la misma sea otra persona. Dichas dimensiones del derecho pueden ser perfectamente cumplidas si son aplicadas a una persona jurídica, por lo que no se advierte razones para negar la titularidad del mismo ni, en consecuencia, limitar su acceso al hábeas data, como mecanismo de tutela en sede de jurisdicción constitucional.[351]

Por tanto, el derecho a la protección de datos personales por su contenido intrínseco puede ser ejercido por personas jurídicas, ya que sus datos propios y distintos de los miembros, personas naturales que los integran, pueden tratados sin su autorización o sin el mandato de la ley, y causar transgresiones a su derecho a la autodeterminación informativa o a otros derechos fundamentales. Es en este sentido que la Corte Constitucional, en sentencia No. 001-14-PO-CC, de 3 de julio de 2014, dicta la siguiente regla de jurisprudencia vinculante obligatoria:

> 3. Por las características del derecho a la protección de datos personales, no se considera constitucionalmente adecuada la limitación a la calidad de las personas jurídicas como

[350] Ibíd., Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 068-10-SEP-CC], ROS No. 372, (27 de enero de 2011).
[351] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 001-2014-PJO-CC].

> titulares del mismo; sin embargo, la información personal de dichos sujetos únicamente se extiende a las personas asociadas o a sus representantes legales, en tanto a la calidad que ostentan respecto de la persona jurídica, con estricto respeto al derecho a la protección de los datos personales y derechos conexos que le son atinentes a su naturaleza.[352]

Si bien esa regla obligatoria determina que pueden ser titulares del derecho a la protección de datos personales las personas jurídicas, puntualiza además que en los datos propios de la persona jurídica también se comprenderá como información personal aquella relativa a personas asociadas o a sus representantes legales.

Al respecto, en las consideraciones y fundamentos de la sentencia que no constituyen regla vinculante se determina que debe entenderse como información personal de la persona jurídica, distinguiéndola de la de sus socios y representantes, aquella referente a la relación o posición, cargo o la relación jurídica establecida con respecto de la persona jurídica, tal como consta en la cita que sigue:

> 29. Ante afirmaciones como las presentadas en esta sentencia cabe, sin embargo, realizar una aclaración importante, atinente a la noción de información «personal». Esta Corte considera imprescindible distinguir entre la información que atañe a la persona jurídica y aquella que puede ser considerada como de dominio de sus asociados, principalmente debido a que en aplicación errónea de la garantía del hábeas data, podría vulnerarse el derecho a la protección de datos e información personal de individuos que, aunque vinculados a la persona jurídica, no son identificables con ella. La tradicional noción del derecho civil, según la cual las personas jurídicas, así como los derechos y obligaciones de las que son titulares son distintos de los que la conforman, puede ser de utilidad para la diferenciación descrita. Si las personas jurídicas tienen el derecho a reclamar por medio del hábeas data actos tendientes a la protección de [...] «datos personales e informes [...] sobre sí misma, o sobre sus bienes...», este derecho solamente puede extenderse a sus socios, representantes legales y personas relacionadas, en tanto la posición que ocupan y la relación jurídica establecida respecto de la persona jurídica, y estrictamente respecto de ellas. No es dable, entonces, que una persona jurídica reclame como suyo el derecho a la protección de datos e información personal de quienes están relacionados con ella, en tanto este derecho solo corresponde a la persona a quien le es atinente, salvo que la exigencia de protección por parte de la persona jurídica se sustente en la debida autorización de sus socios o representantes legales.

Tal como señala la jurisprudencia citada, no queda duda de que deberán protegerse los datos de carácter personal, tanto de las personas jurídicas, como de las personas asociadas y de sus representantes legales en virtud de la existencia de relaciones de pertenencia o representación de la persona jurídica, así como si cada uno por su lado solicita protección. Resta preguntarnos si el término *persona jurídica* incluye a todos los entes ficticios a los que la normativa ecuatoriana reconoce personalidad jurídica, ya que genera dudas la posibilidad de reconocerle titularidad de derechos, especialmente de los constitucionales, a aquellos patrimonios autónomos que nuestra legislación expresamente reconoce personalidad jurídica, como es el caso del patrimonio autónomo producto de un contrato de fideicomiso mercantil; ver el artículo 109 de la Ley de Mercado de Valores.

Ahora bien, en un análisis sistemático y armónico es necesario identificar si en el resto del texto constitucional existen otras referencias al derecho a la protección de datos personales. Al respecto, el numeral 11 del mismo artículo 66 de la CRE acerca del derecho a guardar reserva sobre sus convicciones dice: “En ningún caso se podrá exigir o utilizar sin

[352] Ibíd., 10.

autorización de titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica". Esta norma alude expresamente a datos sensibles que desde el derecho a la protección de datos personales pueden constar en un fichero o base de datos y en tal sentido serían materia de protección, pues solo su titular o su legítimo representante pueden autorizar, exigir o utilizar. La referencia al legítimo representante significa que este derecho solo puede ser solicitado el titular directo del dato. Ahora bien, tal como señala la jurisprudencia vinculante antes citada, sería necesario analizar caso por caso para verificar si los titulares pueden ser personas jurídicas, comunidades, pueblos, nacionalidades o colectivos, en consideración a las posibilidades derivadas de la necesaria materialidad o dignidad del titular del derecho o de su naturaleza social, en un contexto específico, por ejemplo aportes de una persona jurídica o de un colectivo para determinado candidato lo que determina su filiación o pensamiento político.

De otro lado, el artículo 39 de la CRE, que en el Título II, Derechos, Capítulo Tercero, Derechos de las personas y grupos de atención prioritaria, en la Sección Tercera, Movilidad humana, señala en el numeral 5 del artículo 40.- "[...] El Estado, a través de las entidades correspondientes, desarrollará entre otras las siguientes acciones para el ejercicio de los derechos de las personas ecuatorianas en el exterior, cualquiera sea su condición migratoria: [...] 5. Mantendrá la confidencialidad de los datos de carácter personal que se encuentren en los archivos de las instituciones del Ecuador en el exterior". Los titulares a los que se refiere esta norma constitucional son personas físicas en un contexto transfronterizo.

No se menciona al *nasciturus* como sujeto de derechos en la Constitución ecuatoriana, aunque el artículo 45 de la CRE establece que "El Estado reconocerá y garantizará la vida, incluido el cuidado y protección desde la concepción". El reconocimiento de su condición de titular de ciertos derechos consta en los artículos 61 y 63 del Código Civil,[353] no siendo la protección de datos personales uno de los derechos que expresamente se le reconocen.

El artículo 362 de la CRE, que se refiere a la atención de salud como servicio público, señala: "Los servicios de salud serán seguros, de calidad y calidez, y garantizarán el consentimiento informado, el acceso a las información y a la confidencialidad de la información de los pacientes". Los datos de los pacientes, por su naturaleza sensible, serán protegidos con la confidencialidad. En esta norma los titulares son personas naturales que son las únicas que pueden padecer enfermedades, necesitar servicios de atención, y en consecuencia ser denominadas pacientes.

La primera disposición transitoria de la CRE señala que "El órgano legislativo, en el plazo máximo de [...] trescientos sesenta días, se aprobarán las siguientes leyes: [...] 8. Las leyes que organicen los registros de datos, en particular los registros civil, mercantil y de la propiedad. En todos los casos se establecerán sistemas de control cruzados y bases de datos

[353] ASAMBLEA NACIONAL DEL ECUADOR, [Código Civil Codificado, en ROS, No. 46 (24 de junio de 2005), Última modificación: 08 de julio de 2019]: "Artículo 61.- La ley protege la vida del que está por nacer. El juez, en consecuencia, tomará, a petición de cualquiera persona o de oficio, todas las providencias que le parezcan convenientes para proteger la existencia del no nacido, siempre que crea que de algún modo peligra. Toda sanción a la madre, por la cual pudiera peligrar la vida o la salud de la criatura que tiene en su seno, deberá diferirse hasta después del nacimiento. [...] Artículo 63.- Los derechos que corresponderían a la criatura que está en el vientre materno, si hubiese nacido y viviese, estarán suspensos hasta que el nacimiento se efectúe. Y si el nacimiento constituye un principio de existencia, entrará el recién nacido en el goce de dichos derechos, como si hubiese existido al tiempo en que le correspondieron. En el caso del Artículo 60, inciso segundo, pasarán estos derechos a otras personas, como si la criatura no hubiese jamás existido".

nacionales". Aunque no se hace referencia expresa a datos personales, sin embargo por el tipo de bases de datos como son: el registro civil, el registro mercantil y el registro de la propiedad es claro que contienen datos de personas naturales y jurídicas en su relación con el Estado y en ejercicio del derecho de propiedad.

La Ley de Comercio Electrónico y Mensaje de Datos en el artículo 9 establece a las personas como titulares del derecho a la protección de datos personales. En la disposición general 8, en el glosario determina cómo varios términos de la ley deben ser entendidos, señala que los datos personales son "aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley". Del análisis de este texto, se infiere que el titular puede ser una persona natural, pues este tipo es titular de datos íntimos. Ahora bien, esta norma dictada antes de la vigencia de la Constitución de 2008, se encuentra desfasada, ya que la protección de datos personales ahora es un derecho autónomo e independiente de la intimidad. De esta manera, como se analizó en líneas anteriores, también la persona jurídica puede ser titular de este derecho porque se protege la autodeterminación informativa no solo de los datos propios de la esfera íntima, sino de todos aquellos de la persona jurídica y así decida autorizar su recolección, tratamiento o difusión o que pudiera llegarle a causar un perjuicio. En concordancia con el reglamento a esta ley, en su artículo 21 se habla de que se protegerá también los datos de los consumidores; y, conforme señala el artículo 2 de la Ley Orgánica de Defensa al Consumidor, los consumidores serán toda persona natural o jurídica que como destinatario final adquiera, utilice o disfrute bienes o servicios, o bien reciba oferta para ello.

Desde la visión de protección de la seguridad ciudadana, el artículo 14 de la Ley de Seguridad Nacional establece la obtención, sistematización y análisis de la información específica referida a las amenazas, riesgos y conflictos que afecten a la seguridad integral, cuyos datos de personas naturales y jurídicas son materia de análisis.

En el artículo 22 de la Ley de Telecomunicaciones, cuando se refiere a la privacidad y protección de datos personales hace referencia a los abonados, clientes y usuarios, quienes pueden ser personas naturales y jurídicas, quienes conforme el artículo 21 del mismo cuerpo legal son personas naturales o jurídicas consumidoras de servicios de telecomunicaciones.

Por último, resta analizar si la garantía constitucional de *habeas data*, concerniente a la defensa del derecho a la protección de datos personales puede ser interpuesta, tanto por personas naturales como por personas jurídicas. En primer lugar, en virtud del principio de universalización, todos los titulares reconocidos en el artículo 10 de la CRE pueden interponer garantías jurisdiccionales vigentes, conforme lo señala expresamente el artículo 86 referente a las garantías jurisdiccionales de la Constitución cuando señala en su numeral primero: "Cualquier persona, grupo de personas, comunidad, pueblo o nacionalidad podrá proponer las acciones previstas en la Constitución".

Además, el mencionado artículo 92 de la CRE utiliza la expresión *toda persona* que, como se analizó en líneas anteriores, circunscribe personas naturales, jurídicas e incluso los titulares especialmente reconocidos en nuestra Constitución como: comunidad, pueblos, nacionalidades y colectivos. Es más, el artículo 51 de la Ley Orgánica de Garantías y Control Constitucional[354] (en adelante LOGCC) determina, sin lugar a dudas, que "toda persona,

[354] ASAMBLEA NACIONAL DEL ECUADOR, [Ley Orgánica de Garantías y Control Constitucional, Segundo Suplemento, en RO, No. 52 (22 de octubre de 2009)]. ‹http://www.asambleanacional.gob.ec/es/leyes-aprobadas›. Consulta: 18 de febrero de 2018.

natural o jurídica, por sus propios derechos o como representante legitimado para el efecto, podrá interponer una acción de hábeas data".

Además, el mencionado artículo 92 de la CRE señala que puede interponer esta acción toda persona, por sus propios derechos o como representante legitimado para el efecto. De ese modo, las personas naturales pudieran accionarla, por sí mismas o por intermedio de representantes legitimados siempre y cuando sean los directamente relacionados con el derecho en cuestión; así como las personas jurídicas que, acorde a lo señalado en el artículo 1463 del Código Civil, son consideradas incapaces relativos,[355] quienes no solo por su imposibilidad física, sino por disposición legal, no pueden comparecer por sí mismas para presentar acción de *habeas data*, por eso deberán hacerlo mediante sus representantes legitimados siempre que los datos le sean directamente atribuibles.

Los fundamentos y consideraciones de la sentencia No. 001-14-PO-CC, de 3 de julio de 2014, dictada por la Corte Constitucional, materia de análisis, respecto de la legitimación activa para la interposición de esta acción señalan que:

> [...] la regla general es que esta tenga el carácter de abierta, a modo de permitir el mayor campo posible de exigibilidad y un cierto nivel de conciencia social y solidaria ante las vulneraciones a derechos constitucionales. Sin embargo, en el caso del hábeas data, existen derechos en conflicto que pueden verse seriamente lesionados con una disposición que reconozca la legitimación activa abierta. Si no existe un acto de voluntad expreso que permita al legitimado activo comparecer a nombre del titular de los derechos constitucionales, el derecho a la intimidad y otros que dependen de la confidencialidad de la información personal estarían desprotegidos contra el uso malicioso de la acción. Es por ello que el mismo artículo 92 reduce la legitimación activa a "[t]oda persona, por sus propios derechos o como representante legitimado para el efecto...".[356]

En la citada sentencia se ha generado la siguiente regla vinculante que dice: "La legitimación activa para la presentación de la acción de hábeas data requerirá que quien lo haga sea el titular del derecho a la protección de datos personales que se alegue vulnerada, o su representante legitimado para el efecto".

Dado que existían alegaciones respecto de la validez procesal debido a los mecanismos para determinar la legitimación procesal, la misma sentencia dicta otra regla que soluciona estas dificultades prácticas señalando que: "Para acreditar la representación de las personas jurídicas, será suficiente la entrega del documento que la Ley que regule la materia determine como suficiente para considerar iniciadas sus funciones como representante. El juez constitucional, una vez acreditada la representación, deberá tramitar la acción sin que medie excepción sobre el cumplimiento de los requisitos de ley respecto del documento entregado, la que deberá ser dilucidada por los organismos competentes en sede ordinaria".

---

[355] ASAMBLEA NACIONAL DEL ECUADOR, [Código Civil Codificado, en ROS, No. 46 (24 de junio de 2005), Última modificación: 08 de julio de 2019]: "Artículo 1463.- Son absolutamente incapaces los dementes, los impúberes y la (sic) persona sorda que no pueda darse a entender de manera verbal, por escrito o por lengua de señas. Sus actos no surten ni aún obligaciones naturales, y no admiten caución. Son también incapaces los menores adultos, los que se hallan en interdicción de administrar sus bienes, y las personas jurídicas. Pero la incapacidad de estas clases de personas no es absoluta, y sus actos pueden tener valor en ciertas circunstancias y bajo ciertos respectos determinados por las leyes. Además de estas incapacidades hay otras particulares, que consisten en la prohibición que la ley ha impuesto a ciertas personas para ejecutar ciertos actos".

[356] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 001-2014-PJO-CC].

4.3.2.3 Conclusiones

En Ecuador, el artículo 10 de la Constitución establece la universalización de la titularidad de los derechos y garantías constitucionales, pues determina que no solo las personas naturales, sino toda persona, incluida la jurídica, así como los pueblos, nacionalidades, comunidades y colectivos e incluso la naturaleza son titulares de aquellos derechos consagrados en la Constitución y en los instrumentos internacionales. Sin embargo, no todos los derechos pueden ser invocados y ejercitados por aquellos entes colectivos, incluidos la persona jurídica porque depende de la materialidad y de la dignidad del titular.

Respecto del derecho a la protección de datos, es de aquellos que por su naturaleza garantiza derechos no solo a personas individuales, sino también a personas jurídicas e incluso a comunidades, pueblos, nacionalidades y colectivos porque estos titulares, al tener dignidad e identidad propia, buscan reconocimiento y respeto con individuos autónomos e independientes de los individuos que los integran, y por lo tanto deben ser protegidos por el Estado.

Ahora bien, respecto de personas jurídicas y colectivos será el juez constitucional quien establecerá si los datos de los cuales se solicita protección son de aquellos considerados propios y vinculados a su titular. Además, por la naturaleza misma del derecho a la protección de datos personales, deberán estar protegidos todos aquellos titulares cuyos datos pudieran ser recolectados, archivados, procesados, distribuidos o difundidos sin su autorización o sin el mandato de la ley; es decir, aquellas acciones que pudieran causarles un perjuicio directo a su dignidad o por su intermedio violentar otros derechos fundamentales.

En el mismo sentido, la garantía constitucional del *habeas data* se encuentra dispuesta en la normativa constitucional y legal para que sea interpuesta por cualquiera de los titulares reconocidos en la Constitución.

4.3.3 Objeto o bien jurídico: segundo elemento del contenido esencial

Trazada la metodología, es necesario esbozar las ideas y convicciones generalmente generalizadas entre los juristas respecto del bien jurídico del derecho a la protección de datos personales, para determinar los elementos que lo conforman en la normativa ecuatoriana.

4.3.3.1 El bien jurídico protegido

Comprendido que en la descomposición de un derecho, el objeto será el bien jurídico protegido,[357] se distinguen varios derechos y principios que concretan su ejercicio y que, paulatinamente y desde varias sentencias dictadas por el Tribunal Constitucional español, han constituido su perfil con aquellas características que lo definen y permiten distinguirlo de otros derechos. Sobre las especificidades y alcances de este contenido, desde la perspectiva europea, se analizará a profundidad en el capítulo correspondiente. Por el momento y por cuanto es indispensable establecer el estándar de comparación para la adecuada identificación del contenido esencial en Ecuador, a continuación se enlistan los elementos que conforman el bien jurídico protegido del derecho a la protección de datos personales:

[357] M. APARICIO PÉREZ; Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 609.

a) *El derecho de información:* El ciudadano tiene derecho a conocer la existencia, la finalidad de un fichero, quién es su titular y su domicilio.

b) *La autodeterminación informativa:* El ciudadano tiene derecho a negarse a entregar sus datos a un particular e incluso al Estado, si no se justifica la finalidad de la recogida o esta no se encuentra autorizada por la ley. Asimismo, puede negarse a que sus datos sean conservados una vez que su finalidad primigenia ha desaparecido; a que sus datos sean tratados, procesados, cedidos o utilizados para finalidades distintas para las que fueron recogidos originalmente.

   Al respecto, el Tribunal Constitucional español en su STC 254/1993 señala que la utilización de sistemas informáticos se limita en el honor, la intimidad y el pleno ejercicio de los derechos de las personas. Dicho de otro modo, el tratamiento de datos personales no puede vulnerar derechos fundamentales. Así como tiene un contenido negativo de abstención de los titulares de los ficheros y de todos aquellos que pudieran tener contacto con datos personales y su procesamiento, también propone un contenido positivo visibilizado como un haz de garantías que permiten a las personas un control sobre sus datos. En la mayoría de la jurisprudencia española (SSTC 11/1998, FJ4, 94/1998, FJ4 y 202/1999, FJ 2), al derecho a controlar los datos constantes en un fichero o base de datos se lo conoce como *libertad informática*. Pero debido a la necesidad de no limitarse a los datos contenidos en plataformas informáticas, sino a la información personal que pudiera constar en cualquier tipo de técnica de comunicación, también se utiliza el término *autodeterminación informativa*. No debiera utilizarse la forma *intimidad informática*, pues su tutela no se sujeta únicamente a la esfera íntima de las personas. La libertad informática o autodeterminación informativa:

   > [...] es el derecho a controlar la información personal informatizada, con el fin de asegurar la libertad del individuo frente a los peligros derivados de la acumulación de información personal. Su objeto es garantizar la libertad de las personas, entendida como libertad de actuación, de decisión, de participación, etc., es decir, como una libertad de tipo moral. Al situar el acento en asegurar la libertad frente a los riesgos que representan los bancos de datos, se están a la vez garantizando todos los derechos del individuo.[358]

c) *Principios propios del derecho a la protección de datos personales:* Los principios que regulan este derecho y que son parte imprescindible de él como el consentimiento informado, el deber de información, la pertinencia, la calidad de datos, la adecuación del tratamiento a la finalidad autorizada, la seguridad, la confidencialidad y el secreto.

4.3.3.2 El bien jurídico protegido en la normativa ecuatoriana

Del estudio de los antecedentes del reconocimiento a la protección de datos personales en Ecuador, se puede considerar que desde la visión de la búsqueda de la paz del hogar se tiene en cuenta a la privacidad como el elemento unificador a protegerse mediante, por ejemplo, la inviolabilidad del domicilio; del secreto y confidencialidad de las comunicaciones, de la inviolabilidad de la correspondencia; de la honra, imagen y de la intimidad. Si bien todos ellos fueron considerados meros derechos instrumentales, son en realidad derechos autónomos, con un contenido y dimensiones propias.

[358] M. M. SERRANO PÉREZ, *El derecho fundamental a la protección de datos*, 178.

Esta evolución en el reconocimiento de los derechos es una concreción del derecho al libre desarrollo de la personalidad; en otras palabras, de la autodeterminación individual o autoconstrucción social como manifestación de la dignidad humana.[359] Cabe destacar que todos estos derechos antes citados han sido estructurados desde una postura negativa;[360] es decir, desde el deber de abstención de todas las personas que deben respetar el derecho e inhibirse de realizar cualquier acción que perturbe su contenido. En este sentido, la autodeterminación informativa tiene una doble dimensión: un deber de abstención que marca una posición negativa frente al derecho a la protección de datos personales; y además, una posición positiva por la cual el titular del derecho puede decidir en el ejercicio de su libertad individual a quién, en qué circunstancias y bajo qué limitaciones entregar sus datos personales.

Ahora bien, la vigente Constitución de 2008 distingue el derecho de protección de datos personales de otros derechos conexos que fueron directa o indirectamente sus antecedentes inmediatos. Aún más, respecto de la intimidad como antecedente directo, Latinoamérica, y en este caso Ecuador no estuvo exento de la forma inicial de defender a las personas y sus datos, desde esta perspectiva. Sin embargo, como se verificó de los debates realizados por los asambleístas constituyentes, cuando se discutió el contenido del derecho se concluyó que este no se limita en la intimidad, sino que constituye un derecho autónomo e independiente.

Del texto del mencionado artículo, así como de la acción de *habeas data* que permite su garantía constitucional, podemos decir que el bien jurídico de la protección de datos personales se determina en los siguientes derechos:

a) *El derecho de información:* Si bien no consta en el artículo 66 de la Constitución, sí aparece en el artículo 92 de la CRE y en el artículo 49 de la LOGJCC, relativos al *habeas data*, cuando menciona que toda persona tendrá derecho a conocer de la existencia, finalidad, origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

b) *El derecho de acceso:* Que será analizado en el contenido de las facultades que les corresponden a los titulares de un derecho y no como parte del objeto o bien jurídico protegido.

c) *El derecho a la autodeterminación informativa:* Que se manifiesta en la decisión que tiene el titular del derecho sobre la información y datos personales como una de las formas o manifestaciones de su libertad individual en la esfera social. No se refiere solamente a datos personales, sino a información, con lo cual se supera la discusión doctrinaria de si este derecho tiene materialidad únicamente informática o se refiere a cualquier información se encuentre en soporte electrónico o no. Así, este derecho

[359] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 696.

[360] Según Humberto Nogueira Alcalá: "El concepto o noción de regulación desarrollado por la jurisprudencia no es susceptible de aplicarse a los derechos que establecen un contenido de carácter negativo, donde no se garantiza la ejecución de una conducta sino que se establece la prohibición de ella, como ocurre con algunos derechos en nuestra Carta Fundamental, por ejemplo: el no ser objeto de apremios ilegítimos (artículo 19 N×1), la inviolabilidad del hogar (artículo 19 N×5), el no declarar como inculpado bajo juramento sobre hecho propio (artículo 19 N×7, literal f), la no aplicación como sanción de la pérdida de derechos previsionales (artículo 19 N× 7 literal h); ya que estos derechos y garantías no constituyen conductas que pueden sujetarse a formalidades o procedimientos". Ver H. NOGUEIRA ALCALÁ, "Aspectos de una teoría de los derechos fundamentales: la delimitación, regulación, garantías y limitaciones de los derechos fundamentales".

tiene una amplia concepción que incluye información que conste en cualquier técnica de comunicación. El numeral 19 del artículo 66 de la CRE, cuando incluye entre los derechos que son parte de la protección de datos personales a la "decisión sobre información y datos de este carácter", se refiere directamente a la autodeterminación informativa.

Compete analizar la jurisprudencia obligatoria dictada por la Corte Constitucional que, en Sentencia No. 001-14-PO-CC, de 3 de julio de 2014, referente a la acción constitucional de *habeas data* y relativo al derecho a la protección de datos personales, establece como regla vinculante lo siguiente: "2. En el caso de la autodeterminación informativa, como parte del derecho a la protección de datos personales, implica la necesidad de garantizar la protección de la esfera íntima de las personas, así como la posibilidad de ejercer control sobre los datos personales del sujeto, aunque no se encuentren en su poder".

Esta regla de la jurisprudencia vinculante resulta contradictoria porque, pese a registrar a la autodeterminación informativa como elemento sustancial del contenido esencial del derecho a la protección de datos personales y concebirla como aquella que posibilita ejercer control sobre los datos personales, aun de aquellos que no están bajo su poder, pareciera limitar su campo de acción, pues lo circunscribe a los datos de la esfera íntima de las personas. Para esta jurisprudencia, pareciera que el derecho a la autodeterminación solo procede para aquellos datos considerados íntimos; de modo que esta alusión es innecesaria y, lejos de clarificar el derecho del titular respecto de todos los tipos de datos, puede causar confusión.

Dicha aseveración, como ha ocurrido en otros países -entre ellos Argentina en donde se destaca el fallo del Tribunal que exalta respecto a la solicitud de hábeas data que "esta información debe referirse a cuestiones relacionadas con la intimidad"[361] y España cuyo Tribunal Constitucional atendió la efectividad de la autodeterminación informativa como una garantía entregada a la tutela de la intimidad y el honor[362]- dificulta en el ejercicio del derecho debido a la indeterminación en la identificación de aquellos datos que pueden ser considerados íntimos. En la doctrina y la jurisprudencia internacional, la teoría de las esferas ha sido ampliamente superada. Incluso gran parte de los autores entre ellos, Sánchez Urrutia[363] y Carretero[364], consideran que una de las diferencias radicales entre el derecho a la protección de datos personales y el derecho a la intimidad es precisamente incluir en el ámbito de protección a los datos considerados inocuos o irrelevantes; es decir, aquellos que no se encuentran en ninguna de las esferas. A esta teoría se la denomina *teoría del mosaico* porque, utilizando fragmentos de datos o datos irrelevantes, mediante las actuales tecnologías, se puede reconstruir perfiles completos de un individuo, lo que sin duda pudiere afectar el libre desarrollo de la personalidad, su intimidad, honor, imagen, voz y otros derechos fundamentales.

d) *Principios propios del derecho a la protección de datos personales:* El numeral 19 del artículo 66 de la CRE no contiene mención expresa a los principios; sin embargo,

[361] CCont. Adm. 1ª Nom. de Córdoba, 29/3/1995, "Flores, Marcela A. c. Provincia de Córdoba", LLC, 1996-316. AR/JUR/1225/1995.
[362] D. ALTMARK, Tratado de derecho informático, (Buenos Aires: La Ley, 2012), 566.
[363] A. SÁNCHEZ URRUTIA, *Tecnología, Intimidad y Sociedad democrática*, (Barcelona: Icaria, 2003), 35.
[364] S. CARRETERO, *Nueva introducción a la teoría del derecho*, (Madrid: Dykinson, 2010), 172.

señala que el derecho a la protección de datos personales incluye el acceso, la decisión sobre información y datos de este carácter, así como su correspondiente protección. En consecuencia, los principios estarían incluidos en la mención general: "así como su correspondiente protección". De la forma tan general en la que está dispuesto este texto, se puede considerar que la norma los incluye, ya que los principios de información, calidad, finalidad, seguridad, entre otros, son elementos fundamentales porque permiten una real y efectiva protección de los datos personales. Y aunque no constan expresamente detallados en el texto constitucional, son parte de su contenido esencial porque solo puede efectivizarse una debida protección de los datos personales de los ciudadanos si se cumplimentan. A manera de ejemplo, el artículo 92 de la CRE, sobre el *habeas data*, hace referencia al principio de seguridad, aunque mencionando exclusivamente datos sensibles. En Ecuador algunas normas específicas invocan estos principios e incluso desarrollan varios de ellos;[365] no obstante, deben tratarse en un texto específico y pertinente que unifique su contenido, aclare contradicciones y llenen lagunas normativas.

e) *Principio de consentimiento informado:* Es uno de los principios que aparece expresamente registrado en el texto constitucional, pues la recolección, archivo, procesamiento, distribución o difusión de datos o información personal requerirán siempre la autorización del titular. Aunque este consentimiento tiene como única limitante el mandato de ley, cuando por razones legítimas de interés general sea necesario recabar esos datos. Pero la norma no hace mención a si este consentimiento debe cumplir con el requisito previo de ser obtenido con suficiente información que permita obtener una voluntad plena sin vicios con total conocimiento de las ventajas o desventajas, beneficios o amenazas, etc. Esta condición fundamental debe constar en una ley, porque es parte del contenido esencial del derecho que garantiza su ejercicio.

f) Principio de finalidad: Si bien este principio no consta recogido en el numeral 19 del artículo 66 de la CRE, sí puede visibilizarse en el artículo 92 de la CRE cuando señala

[365] Ver Ecuador, *Reglamento a la Ley del Sistema Nacional de Registro de Datos Públicos*, en ROS, No. 718 (23 de marzo de 2016):

> Artículo 11.- Principios para el tratamiento de datos personales.- Todo tratamiento de datos públicos que se haga por parte de la Dirección Nacional de Registro de Datos Públicos, de las instituciones que componen el Sistema Nacional de Registro de Datos Públicos, y en general, por las personas naturales o jurídicas, públicas o privadas, que mantuvieren o administren por disposición legal información registral de carácter público, deberá observar los siguientes principios:
> 1. Principio de veracidad o calidad de los datos personales.- La información contenida en los registros o bases de datos públicos o privados debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
> 2. Principio de finalidad.- El tratamiento de datos personales debe responder a una finalidad legítima, de acuerdo a la Constitución de la República y la Ley.
> 3. Principio de utilidad.- El acopio, procesamiento y divulgación de los datos personales deben cumplir una función determinada que sirva a la finalidad que persiga el registro del dato.
> 4. Principio de incorporación.- Cuando de la inclusión de datos personales en determinadas bases se deriven situaciones ventajosas para el titular, la entidad administradora de datos estará en la obligación de incorporarlos, si el titular reúne los requisitos que el orden jurídico exige para tales efectos, de tal forma que queda prohibido negar la incorporación injustificada a la base de datos.
> 5. Principio de rectificabilidad.- Los datos públicos registrados son susceptibles de rectificación o supresión en los casos y con los requisitos previstos por la Ley y el presente Reglamento.
> 6. Principio de responsabilidad.- La responsabilidad sobre la veracidad y autenticidad de los datos registrales, es responsabilidad del declarante, cuando éste provea la información; sin perjuicio de los mecanismos de verificación que implemente la Institución ante quien se efectúe la declaración.

que las personas tendrán derecho a conocer el uso y la finalidad de sus datos personales. Pese a que la referencia es parte del derecho a ser informado, dicha mención reconoce como fundamental para la protección de los datos al principio de finalidad, ya que la pertinencia, legitimidad en la recogida y uso de la información permite una protección integral del derecho. Asimismo, el artículo 11 del Reglamento a la Ley del Sistema Nacional de Registro de Datos Públicos señala al principio de finalidad como uno de los aplicables en el tratamiento de datos personales que se hagan por parte de la Dirección Nacional de Registro de Datos Públicos, de las instituciones que componen el Sistema Nacional de Registro de Datos Públicos, y en general, por las personas naturales o jurídicas, públicas o privadas, que mantuvieren o administren por disposición legal información registral de carácter público.

g) *Principio de seguridad:* Este principio consta reconocido únicamente para el caso de datos sensibles, que por su naturaleza deben ser autorizados por el titular o por la ley y a los que es indispensable aplicar medidas de seguridad, conforme señala el artículo 92 de la CRE.

4.3.4 Contenido de las facultades que les corresponden a los titulares para el ejercicio de ese objeto

En el análisis de contenido esencial del derecho a la protección de datos personales es menester analizar ahora el contenido de un derecho, entendido como la especificación jurídica del objeto; consiste en el conjunto de facultades que se atribuyen al titular, las prohibiciones de terceros y la capacidad de reacción del titular del derecho frente al incumplimiento de esas prohibiciones.[366]

4.3.4.1 Contenido de las facultades

La doctrina, la jurisprudencia y la normativa de la mayoría de los países que han regulado el derecho a la protección de datos personales han atribuido como facultades de los titulares del derecho a la protección de datos personales a los denominados derechos ARCO; así como a otros que provienen como consecuencia de su ejercicio y que constan a continuación:

a) Derecho de acceso, rectificación, cancelación y oposición (ARCO). Se entiende al derecho de acceso como aquel que permite comprobar si se dispone de información sobre uno mismo y su origen y finalidad de su tratamiento, conservación y cesión.[367] Por su parte, los casos de inexactitud, carencia, incompletitud se solucionan a través de la rectificación.[368] Mientras que la cancelación procede cuando "los datos son innecesarios para la finalidad del fichero o sean excesivos en relación con la misma"[369] y por lo tanto es menester anular, borrar, hacer ilegible, destruir o dejar irreconocibles los datos. Finalmente, la oposición consiste en "el derecho del interesado a negarse, por motivos legítimos, a que sus datos personales sean objeto de tratamiento".[370]

[366] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 609.
[367] P. L. MURILLO DE LA CUEVA, "El Derecho a la autodeterminación informativa", 187.
[368] M. M. SERRANO PÉREZ, *El derecho fundamental a la protección de datos*, 358.
[369] A. I. HERRÁN ORTIZ, *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales* (Madrid: Dykinson, 2002), 288.
[370] A. A. SÁNCHEZ BRAVO, *La protección del derecho a la libertad informática en la Unión Europea* (Sevilla: Universidad de Sevilla, 1998), 97.

b) Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales.[371]
c) Derecho de consulta al registro general de protección de datos personales.[372]
d) Derecho a indemnización por daños causados.[373]

4.3.4.2 Contenido de las facultades en la normativa ecuatoriana

Con la finalidad de identificar el contenido del derecho a la protección de datos personales desde el conjunto de facultades propias de sus titulares, las prohibiciones de terceros y las consecuencias de los incumplimientos de estas prohibiciones, analizaremos dos normas que se complementan: el numeral 19 del artículo 66 y el artículo 92 de la CRE. El primero establece el derecho fundamental y el segundo recoge la garantía del *habeas data*, mecanismo constitucional de tutela de este derecho y de otros como la intimidad, al honor, el buen nombre, la imagen, la propia voz, a los que completa e integra, por ser parte de la estructura de su sistema de protección.

a) *Derecho de acceso, rectificación, cancelación y oposición (ARCO):* De la simple lectura del numeral 19 del artículo 66 de la CRE podemos identificar al derecho de acceso, pero no encontramos mención alguna sobre los otros derechos como el de rectificación, cancelación y oposición. La norma en mención señala que el derecho a la protección de datos personales incluye el acceso, la decisión sobre información y datos de este carácter, así como su correspondiente protección. Entonces, se puede afirmar que los otros derechos están incluidos en la parte que, de forma general, menciona: *así como su correspondiente protección*. En esta generalización pudiera comprenderse que se encuentran incluidos los derechos como el de rectificación, cancelación e incluso el de oposición, que son derechos o facultades indispensables para el ejercicio del derecho a la protección de datos, pues permiten su efectiva vigencia y materializan su eficacia real.

   Al igual que lo ha hecho Latinoamérica, la norma que otorga la mayoría de las facultades descritas en los derechos ARCO es aquella que consagra la garantía constitucional del *habeas data*, artículo 92 de la CRE y 49 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (en adelante LOGJCC), publicada en Registro Oficial Suplemento No. 52, de 22 de octubre de 2009, que en texto casi

[371] Ver DIRECTIVA 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, Luxemburgo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos: "Artículo 15. Decisiones individuales automatizadas 1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.".

[372] Ver España, LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. "Artículo 14. Derecho de consulta al Registro General de Protección de Datos. Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita".

[373] Ver España, LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. "Artículo 19. Derecho a indemnización. 1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. 2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria".

idéntico se refiere al derecho de las personas a "acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas, en soporte material o electrónico". Asimismo, el artículo 50, al referirse al ámbito de protección del *habeas data*, precisamente señala el caso de la negativa de acceso. Como se analizó en líneas anteriores, el *habeas data* tanto en la norma constitucional como en la legal hace énfasis en el derecho de acceso, señalando que esta garantía jurisdiccional podrá solicitarse respecto de aquella información expresamente descrita en la norma citada.

Asimismo, en el artículo 92 de la CRE y artículo 49 de la LOGJCC, en textos muy similares, determinan que: "La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación…". Por su parte, el artículo 50 de la LOGJCC señala que se podrá interponer *habeas data* "cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos".

Como vemos del análisis de las normas, la garantía constitucional del *habeas data* reconoce casi todos los derechos ARCO, excepto el de oposición. Anotándose que, para que prospere la acción deberá probarse que los datos personales son erróneos o afectan derechos, elementos adicionales que no constan en la versión constitucional y que limitan su procedencia. Finalmente, merece especial mención que la gratuidad del acceso se encuentra reconocida a nivel constitucional y legal como garantía eficaz para la interposición de esta acción, que además permite su real aplicación.

Por su parte, el artículo 49 de la LOGJCC completa el sistema de protección al mencionar que "no podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos", ya que en estos casos el interés general prima por encima de los derechos de los particulares, sobre todo en ámbitos como seguridad, salud pública, educación o registro ciudadano de ciudadanía y empadronamiento, por ejemplo.

Es pertinente diferenciar el derecho de acceso constante en la acción de *habeas data*, como mecanismo de tutela del derecho a la protección de datos personales, del derecho de acceso a la información pública. La Constitución de la República del Ecuador previó la existencia de una garantía jurisdiccional particular, denominada acceso a la información pública, que consta en el artículo 91 de la CRE y en el artículo 47 de la LOGJCC y que tiene por finalidad autorizar a los ciudadanos el libre acceso a la información pública, que es aquella generada por entidades públicas o privadas que manejen fondos del Estado o realizan funciones o servicios públicos y a las que se aplica en general el principio de publicidad de la información. El objetivo de esta acción es facilitar la participación ciudadana, la toma de decisiones de interés general y la rendición de cuentas como mecanismos para alcanzar la democracia, la publicidad y la transparencia en el manejo de los intereses y recursos públicos.

En cambio, los datos personales se resguardan desde la visión de la confidencialidad, por su primigenio origen relacionado con la intimidad, la privacidad, el honor, el libre desarrollo de la personalidad y, además, porque la autodeterminación informativa resulta parte del bien jurídico a ser protegido. Únicamente se rompería el principio de

confidencialidad por autorización del titular o por mandato de ley, debidamente justificado por razones de interés público, como por ejemplo: grave peligro para la vida o la salud de la población; en estos casos, los datos de los ciudadanos podrían ser recogidos contra su voluntad y aún más dispuestos como accesibles al público. En este sentido, el artículo 66, numeral 19 y también el artículo 92 de la CRE hacen alusión a que la información archivada solo podrá ser difundida con autorización previa del titular o cuando lo disponga la ley.

El mandato legal es indispensable no solo para la recogida de datos, sino para su archivo y permanencia en ficheros regentados por instituciones públicas, así como para determinar si son de aquellos que deben o no ser accesibles al público. En este sentido, los límites externos de la norma serán aquellas referencias legales que establezcan los casos por los cuales un dato personal debe ser recogido, tratado o publicitado.

Coincidente con esta postura, la Ley de Telecomunicaciones, cuando se refiere al secreto de las comunicaciones y protección de datos personales, en el artículo 77 señala: "Interceptaciones [...] Los contenidos de las comunicaciones y los datos personales que se obtengan como resultado de una orden de interceptación legal estarán sujetos a los protocolos y reglas de confidencialidad que establezca el ordenamiento jurídico vigente". Se infiere que la confidencialidad es la garantía, por tanto, incluso en ejercicio de una orden de interceptación legal de datos personales, se deberá respetar este secretismo mediante protocolos y reglas que garanticen este derecho.

b) *Derecho a impugnar valoraciones automatizadas:* Respecto del derecho de las personas a no soportar valoraciones, producto de procesos automatizados que afecten derechos fundamentales, no existe mención expresa en ninguna de las normas constitucionales citadas. Ahora bien, el numeral 3 del artículo 50 de la LOGJCC establece que podrá interponerse *habeas data* "cuando se dé un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente".

   Si bien la norma no invoca a los procesos automatizados, en cambio sí reconoce que la información personal puede ser utilizada para transgredir derechos constitucionales, y en este sentido es procedente la interposición de la acción de *habeas data*. Únicamente se exceptúan dos casos: i) cuando exista expresa autorización, pero no se especifica si el asentimiento proviene de la persona o de la ley. Si proviene de la persona sería un contrasentido que el individuo facultare voluntariamente un uso de datos personales que directamente le signifique una vulneración a un derecho del que es titular irrenunciable, por lo que la autorización proviene de la ley. La ponderación de derechos lo realiza el legislador, quien determina, a nivel legal, cuándo se puede utilizar el dato de una persona, de tal forma que pudiera causarle un perjuicio a sus derechos fundamentales, pero este daño se encuentre justificado en un bienestar mayor o colectivo; asimismo, ii) cuando exista orden judicial, la cual deberá estar debidamente motivada.

c) *Derecho de consulta:* Respecto de los derechos de consulta al registro general de protección de datos personales, no existe en Ecuador una ley de protección de datos que establezca la obligatoriedad de realizar registro de estos ficheros. Es más, la

acción de *habeas data* está diseñada para que cada persona pueda solicitar directamente al responsable del fichero información respecto de la existencia, tratamientos y finalidades de los datos de carácter personal. Esto sin duda plantea una dificultad práctica, en la medida de que muchas veces se desconoce quién es el responsable del tratamiento, y en consecuencia en contra de quién debe interponerse la acción. Además, la ausencia de registro impide: un control preventivo que evite transgresiones a derechos fundamentales; la corroboración de que la información entregada por el demandado es verídica, completa o actualizada; y la imposibilidad de implementar medios técnicos adecuados que faciliten el seguimiento y la identificación de vulnerabilidades en los sistemas.

De otro lado, la Ley del Sistema de Registro de Datos Públicos (en adelante LSRDP), en el artículo 13 señala que: el Registro Civil, de la Propiedad, Mercantil, Societario, Vehicular, de naves y aeronaves, patentes, de propiedad intelectual, registros de datos crediticios y los que en la actualidad o en el futuro determine la Dirección Nacional de Registro de Datos Públicos serán parte del sistema de registro de datos públicos, y por lo tanto deberán regirse a las disposiciones sobre seguridad, organización, sistematización, interconexión, eficacia y eficiencia de su manejo, publicidad, transparencia, acceso e implementación de nuevas tecnologías; así como de integridad, protección y control de la información, de tal forma que los responsables de los ficheros respondan por la veracidad, autenticidad, custodia y debida conservación de los registros (artículo 4 de la LSRDP). Si bien estos registros contienen datos personales que conformarían parte del sistema y que deben estar a disposición de sus titulares para que estos puedan hacer efectivos sus derechos ARCO, no tienen por finalidad facilitar al órgano especializado de protección ni tampoco al individuo, información respecto del responsable, el tratamiento o finalidad de cada fichero para que pueda hacer uso de las acciones que considere pertinentes.

d) *Derecho a solicitar indemnizaciones:* Finalmente, respecto del derecho a solicitar indemnización por los daños causados, tanto el artículo 92 de la CRE como el artículo 49 de la LOGJCC establecen que la persona afectada podrá demandar por los perjuicios ocasionados cuando los derechos de acceso, rectificación, eliminación o anulación no hayan sido respetados o cuando los principios de finalidad, seguridad y calidad de la información no se cumpla por parte de los responsables de los ficheros. Cabe anotar que la norma constitucional se limita al señalar el derecho a solicitar indemnizaciones, mientras que la norma legal amplía esta protección, pues faculta la reparación integral. Este tema se analizará a profundidad en el título pertinente de este trabajo doctoral.

4.3.5 Sujetos pasivos u obligados

Hemos llegado al último de los elementos que permite identificar el contenido esencial de un derecho, que consiste en determinar cuáles son los sujetos pasivos u obligados a respetar el derecho a la protección de datos personales.

4.3.5.1 Sujetos pasivos u obligados

Tanto la Directiva 95/46 de 24 de octubre[374], como el vigente RGPD, identifican, sin cambios sustanciales, a quienes debe considerarse como sujetos pasivos u obligados.

Además establecen que los sujetos pasivos son aquellos a quienes se solicita el cumplimiento las medidas técnicas y organizativas que permitan garantizar y acreditar que el tratamiento es conforme al RGPD, a las leyes de cada país y a la legislación sectorial aplicable. Son aquellos que deben garantizar que los derechos de los titulares no se vean transgredidos por sus actuaciones en relación con el tratamiento de datos personales a su cargo y además deben responder a la interposición de derechos de acceso, rectificación, supresión u oposición que interpongan titulares de datos personales. De forma que, de no cumplir con sus responsabilidades o causar daño en el tratamiento de los datos personales a su cargo serán responsables, por su acción u omisión, de los daños y por ende de las reparaciones e indemnizaciones causadas.

El RGPD define los sujetos pasivos del tratamiento de datos personales, así como los identifica las características que definen a cada uno de los sujetos pasivos, de tal forma que puedan identificar el nivel de responsabilidad y las obligaciones o deberes particulares o específicos que cada uno debe cumplir, mientras que, el vigente LOPD-GDD español desarrolla estos parámetros generales para su aplicación específica a casos concretos.

Los sujetos pasivos reconocidos en el RGPD y desarrollados en el LOPD-GDD son: el responsable, el encargado del tratamiento, el tercero y el destinario.

a) *Responsable de tratamiento*: El artículo 4, numeral 7) del RGPD determina que es "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento".

b) *Encargado del tratamiento:* El artículo 4, numeral 8) del RGPD señala que es "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

c) Destinatario: El artículo 4, numeral 9) del RGPD establece que es: "la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos

[374] DIRECTIVA 95/46/CE, Luxemburgo:
"Artículo 2: Definiciones: A efectos de la presente Directiva, se entenderá por: (...) d) «responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;
e) «encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;
f) «tercero»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;
g) «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios (...)".

personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento".

d) Tercero: El artículo 4, numeral 9) del RGPD que establece que es: *"*la persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado".

Entre el RGPD y la Directiva 95/46 de 24 de octubre, respecto de los sujetos pasivos casi no existen cambios en lo relativo a las definiciones establecidas en dichas normativas.

Ahora bien, a efectos de este análisis general, cabe aclarar que el encargado de tratamiento tienen una responsabilidad que no es directa, por cuanto actúa por cuenta del responsable del fichero, al que se encuentra vinculado en virtud de una relación contractual, y por tanto, no tiene capacidad para decidir sobre los datos que recoge, los tratamientos que realiza, la finalidad a la que los destina,[375] sino que debe limitarse a cumplir lo dispuesto en el contrato. Sin embargo, tanto en el RGPD[376] como en la LOPD-GDD[377] determinan que al encargado le será aplicable el régimen de responsable cuando trate datos personales para su propia finalidad.

En cuanto a la definición de tercero, esta es idéntica entre la dispuesta el RGPD y la Directiva 95/46 de 24 de octubre. Ahora bien, es la LOPD-GDD española la que determina en su artículo 73 "que será una infracción grave y prescribirá en dos años: " k) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679". Con lo cual la identificación del tercero adquiere importancia para determinar omisiones del responsable del tratamiento sobre todo en cuanto a la inadecuada cesión de datos personales.

Finalmente, en el caso del destinatario la definición es muy similar entre el dispuesto en el RGPD y la Directiva 95/46 de 24 de octubre, añadiéndose que le será atribuible algún nivel de responsabilidad en la medida en la que realice actividades distintas a las señaladas por el

[375] I. SUBIZA PÉREZ Y M. ARIAS POU, *La protección de datos y sus mundos* (Pamplona: DAPP, 2009), 66.

[376] Europa: REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PERSONALES: "Artículo 28 numeral 10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento".

[377] España: LEY ORGÁNICA 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales LOPD-GDD: "Artículo 33.2 que el encargado: "tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público. Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades".

contrato o la ley, y nuevamente el sujeto obligado seguirá siendo el responsable del tratamiento.

4.3.5.2 Sujetos pasivos u obligados en la normativa ecuatoriana

Respecto de la identificación de los sujetos pasivos u obligados del derecho a la protección de datos en Ecuador, el numeral 19 del artículo 66 de la CRE no señala manifiestamente quiénes serían estos; sin embargo, por la forma de redacción se atribuye esta obligación a toda persona que recolecte, archive procese, distribuya o difunda datos o información ya sea que la haya obtenido por la voluntad de sus titulares o por disposición legal. No se hace alusión alguna a la característica fundamental del responsable de un fichero en la mayoría de normativa internacional que es la relativa a su capacidad de decisión.

Por su parte, el artículo 92 de la CRE señala que el *habeas data* procede cuando existan "datos genéticos, documentos, bancos o archivos de datos personales e informes sobre sí mismos o sobre sus bienes que consten en entidades públicas o privadas [...]".

Será sujeto pasivo u obligado del derecho a la protección de datos personales en Ecuador, toda persona privada o pública que tenga documentos, datos genéticos, bancos o archivos de datos personales e informe sobre sí misma o sobre sus bienes. Los artículos 49 y 50 de la LOGJCC establecen como sujetos pasivos no solo a las entidades públicas o privadas, sino que además incluyen a las personas naturales, todos a quienes denomina en su conjunto como responsables del archivo o banco de datos.

Se utiliza la frase persona responsable, en el mencionado artículo 92 de la CRE, para referirse a que serán estas las que podrán difundir información archiva con autorización de su titular o de la ley. La utilización del término responsable manifiesta una carga intrínseca, pues su nombre en sí mismo describe un deber u obligación de abstención y respeto, por la sola condición de tener bajo su tutela datos personales de terceros.

Esos sujetos se constituyen en obligados desde la perspectiva de que, desde una dimensión negativa, deben respetar o abstenerse de transgredir tanto al bien jurídico protegido, como al contenido del derecho a la protección de datos personales.

Respecto al tipo de soporte que puede estar en manos de un administrador público o particular de un fichero, se hace hincapié en que este puede estar en formato físico o electrónico.

Respecto de los sujetos obligados, el artículo 4 de la Ley del Sistema Nacional de Registro de datos Públicos, Ley 0, Registro Oficial Suplemento 162, de 31 de marzo de 2010, última modificación (03-dic-2012), expresamente señala: "Responsabilidad de la información.- Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos [...]". En esta norma se evidencia que el verbo rector que atribuye responsabilidad es *administrar*; es decir, quien organiza, dirige u ordena y en este sentido quien decide sobre los datos. Criterio que, aunque no consta en la normativa constitucional, aparece en la legal y coincide con la visión europea.

El artículo innumerado a continuación del artículo 4 de la misma ley señala a la Superintendencia y a la Dirección Nacional de Registro de Datos Públicos, como obligados indirectos, cuando el titular del dato crediticio exija rectificación de la información ilegal,

inexacta o errónea, pues obliga a comunicar a la Superintendencia respectiva y esta a su vez a la Dirección Nacional de Registro de Datos Públicos, para la actualización del Registro de Datos Crediticios y su difusión a quienes hayan recibido la información errónea. La denominación de obligados indirectos resulta una particularidad de la normativa ecuatoriana, cuyo concepto puede coincidir con el de tercero o destinatario de la normativa europea.

En la Ley de Telecomunicaciones, en el numeral 14 del artículo 24, constan como obligados los prestadores de servicios de telecomunicaciones, ya que deberán adoptar las medidas necesarias para la protección de los datos personales de sus usuarios y abonados, de conformidad con esta ley, su reglamento general y las normas técnicas y regulaciones respectivas.

Como sujetos pasivos adicionales, en la misma Ley de Telecomunicaciones, artículo 85, se describe como obligado adicional a la Agencia de Regulación y Control de las Telecomunicaciones, pues establecerá y reglamentará los mecanismos para supervisar el cumplimiento de las obligaciones, tanto de secreto de las comunicaciones como de seguridad de datos personales; y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para las y los prestadores de servicios, con el fin de que adopten determinadas medidas relativas a la integridad y seguridad de las redes y servicios. De esta manera, es en una Ley de Telecomunicaciones y para el ámbito exclusivo de esta norma que se establece un ente con competencias de regulación de este derecho, conforme señala el numeral 28 del artículo 144 que, entre sus facultades, determina: "Establecer las regulaciones necesarias para garantizar la seguridad de las comunicaciones y la protección de datos personales".

Asimismo, la Ordenanza que regula el uso de las tecnologías de la información y la comunicación en el Municipio del Distrito Metropolitano de Quito, Ordenanza Metropolitana de Quito No. 0159, de 14 de octubre de 2005, en el artículo 5, Datos Personales, señala que "Es obligación de las autoridades municipales correspondientes garantizar la confidencialidad de los datos personales contenido en archivos, registros y bancos de datos municipales".

Como podemos evidenciar de las normas transcritas, cada ley identifica a responsables directos: administradores de ficheros, y a responsables indirectos: aquellos que en virtud de la ley deben establecer el marco regulador que afiance la protección del derecho fundamental a la protección de datos personales o que manejen datos en su condición de destinatarios de los datos o de terceros, aunque sin mencionar esta condición expresamente.

4.3.6 Institucionalidad de protección

En la norma constitucional que reconoce el derecho fundamental a la protección de datos personales y el *habeas data*, no consta determinada la institucionalidad de protección, así como tampoco la norma legal que regula la garantía constitucional la contempla.

Ahora bien, existen normas sectoriales que establecen a varias entidades a distintos niveles de protección dependiendo del ámbito de aplicación. Sobre este particular, se analizará a profundidad en el capítulo quinto de esta tesis doctoral.

4.3.7 Régimen Sancionador

En general, la normativa ecuatoriana ante la existencia de un hecho dañoso, y dependiendo de la conducta perpetrada, puede establecer responsabilidades civiles, penales y administrativas; aun así, no existe un régimen sancionador específico, sino que se deben utilizar los criterios y principios generales de la responsabilidad. Acerca de responsabilidades y regímenes sancionadores, existen varias normas sectoriales que establecen, en sus específicos ámbitos de aplicación, varias conductas lesivas que pudieran generar responsabilidad. Al respecto, se analizará este tema a profundidad en el capítulo de este trabajo de titulación doctoral.

Existe solo una variante proveniente del *habeas data*, pues por su intermedio se puede obtener la reparación integral de un derecho constitucional transgredido. Sobre este tema, se analizará a profundidad en el numeral 6 de este capítulo.

4.3.8 Transferencia internacional de datos

Sobre la temática de transferencia internacional de datos no existe normativa constitucional o legal de carácter general; tampoco referencia alguna en las normas sectoriales dictadas para proteger este derecho en ámbitos específicos.

Puede verificarse, entonces, la necesidad de concienciar en la sociedad ecuatoriana el potencial económico de los datos personales adecuadamente tratado; de modo que pueda establecerse dentro de las prioridades en las relaciones internacionales la posibilidad de conseguir un nivel adecuado de protección que permita un mejoramiento en las interrelaciones y apertura de la economía del Ecuador, especialmente con el mercado europeo.

5. *Habeas data*, garantía jurisdiccional

En el caso ecuatoriano, para determinar el contenido esencial del derecho a la protección de datos personales es indispensable analizar la garantía constitucional del *habeas data*; dado que, conforme se señaló en líneas anteriores, constan descritos en el artículo 92 de la Constitución, relativo a esta garantía constitucional: parte del bien jurídico protegido y de las facultades de sus titulares (derecho de acceso, rectificación, cancelación y anulación).

Además de la pertinente revisión normativa y bibliográfica, para este análisis se desarrolló un proyecto de investigación sobre la aplicación del derecho a la protección de datos y del *habeas data* en la jurisprudencia constitucional, desde 1996 al 2019.[378]

Respecto de la etimología del *habeas data*, "significa «conservar o guardar los datos», o con mayor propiedad como lo señala Morogana Díaz citando a Otón Sidow «que tengas los registros, los datos», habiéndose puesto de resalto su similitud con el hábeas corpus. Se ha hecho notar que a semejanza de este último instituto, en el que se impetra la presentación del «cuerpo» del privado de su libertad para investigar los motivos de la misma, y en su caso disponer la cesación de ese estado, en el hábeas data se requiere se presenten los datos para la verificación de su exactitud, actualidad, etc., a efecto de exigir si correspondiere, su

[378] La autora de esta tesis doctoral lideró este proceso de investigación que contó con la participación de Daniela Macías Villarreal como coordinadora y de los estudiantes del curso de Derecho Informático, Der 903-2 del período académico 2015-1, que va desde septiembre de 2014 hasta febrero de 2015.

inmediata rectificación, actualización, sometimiento a confidencialidad, reserva, etc."[379] De este concepto, resalta su similitud con el *habeas corpus* y se deduce su espíritu, ya que esta garantía constitucional considera que puede evitarse, prolongarse o anularse la transgresión de la dignidad de los titulares de los datos, pues obliga a los sujetos pasivos a presentarse y mostrar los datos para que estos pudieran ser revisados y corregidos de ser el caso.

Si bien se consideraba al *habeas data* como un *derecho – garantía procesal constitucional*, cuyo origen pretendía contrarrestar los peligros de la automatización de la información, como respuesta al desarrollo tecnológico y al tratamiento de datos e información personal. Sin embargo, "como una respuesta a ese desarrollo del poder informático, es una garantía especial que protege, fundamentalmente, el derecho a la intimidad. Como bien dice Ekmekdjian y Calogero Pizzolo, «el derecho a la privacidad o a la intimidad es una consecuencia o derivación del derecho a la dignidad»".[380] Es decir, no se concebía al *habeas data* como manifestación directa del derecho a la protección de datos personales, sino como tutela del derecho a la intimidad y a la privacidad familiar y personal que se consideraba era el bien jurídico violentado por las nuevas tecnologías de la información y comunicación.

Entonces, cuando se identificó que la utilización inadecuada de los datos personales no solo transgredía estos derechos tradicionales, sino que causaba perjuicio a las libertades informativas del individuo, apareció un nuevo derecho denominado protección de datos personales del cual el *habeas data* se constituía ahora en su mecanismo de tutela. Esto es:

> […] la construcción de este nuevo derecho fundamental excede la tradición jurídica que tuvo el derecho a la intimidad, permitiendo que toda información que concierna a cualquier persona pueda ser controlada por él mismo como un freno al poder informático [...] En pocas palabras, el derecho a la libre disposición de los datos personales supone recrear un derecho fundamental que, derivado del derecho a la vida privada del hombre, le permite resolver por sí mismo el tratamiento que quiera asignar a los datos que sobre su persona se almacenen con destino diferentes. La garantía específica para salvaguardar el derecho es el proceso constitucional de hábeas data.[381]

Conforme las primeras Constituciones latinoamericanas, se relacionó estrechamente a esta garantía constitucional principalmente con el derecho a la intimidad; sin embargo, las transgresiones que en el ámbito de lo informático se manifestaron mediante la captación y uso de datos en bancos de datos e informes sobre sí mismos y sus bienes, que por erróneos o desactualizados afectaren ilegítimamente derechos de las personas, generaron que el *habeas data* adquiriere un contenido más amplio que incluye, no solo a la intimidad, a la privacidad personal y familiar, sino a otros derechos fundamentales. Por eso, se afirma que fue constituido para conseguir el amparo prometido a la "generosa tutela judicial prometida a los derechos derivados de la vida privada (intimidad y privacidad)",[382] aunque paulatinamente este ámbito se habría extendido.

En consecuencia, el *habeas data* es una garantía jurisdiccional que pertenece a las garantías constitucionales, por la cual los ciudadanos tienen derecho a verificar que los datos que se encuentran en los ficheros de terceros se encuentren actualizados, completos, correctos y que, de no ser así, puedan ejercitar los derechos de rectificación, actualización o cancelación; en

[379] G. PEYRANO, *Régimen legal de los datos personales y hábeas data* (Buenos Aires: Lexis Nexis DePalma, 2002), 284.
[380] R. CESARIO, *Hábeas Data* (Buenos Aires: Editorial Universidad, 2001), 110.
[381] O. GOZAÍNI, *Hábeas Data, protección de datos personales*, 57.
[382] O. GOZAÍNI, *Hábeas Data, protección de datos personales*, 56.

otras palabras, es un derecho de control sobre sus datos, con lo cual se protegen, no solo el derecho a la protección de datos personales o autodeterminación informativa, sino también otros derechos como la intimidad, la privacidad, la honra, la buena reputación, la identidad, la imagen, la voz, el libre desarrollo de la personalidad, entre otros.

En el caso del Ecuador, el *habeas data* nunca tuvo exclusivamente una finalidad instrumental, sino que, por el contrario, su objetivo también era sustantivo, pues estructuraba las bases del sistema de protección de los derechos constitucionales, inicialmente la intimidad y el honor, posteriormente, la protección de datos personales, la imagen y la propia voz, entre otros. Aunque en líneas anteriores se hizo referencia a estos, para continuar con el análisis se revisará la evolución histórica de esta figura procesal constitucional en Ecuador, con la finalidad de evaluar su histórico y actual contenido esencial que permita completar el estudio del derecho fundamental a la protección de datos personales.

5.1 El *habeas data* en la normativa ecuatoriana: reformas de 1996 y Constitución de 1998

Las reformas a la Constitución de 1996 incorporan por primera vez en una Constitución ecuatoriana al *habeas data*. La norma en referencia se incluyó en la sección II, bajo el título De las Garantías de los Derechos, en el parágrafo III, titulado *Habeas data* con el siguiente texto:

> Artículo 30.- Toda persona tiene derecho a acceder a los documentos, banco de datos e informes que sobre sí misma o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su finalidad. Igualmente, podrá solicitar ante el funcionario o juez competente la actualización, rectificación, eliminación o anulación de aquellos si fueren erróneos o afectaren ilegítimamente sus derechos. Se exceptúan los documentos reservados por razones de seguridad nacional.

Posteriormente, la Asamblea Nacional Constituyente, el 5 de mayo de 1998 expidió la Constitución de 1998, en cuyo capítulo VI, De las Garantías de los Derechos, en la sección segunda Del *Habeas Data*, artículo 94, determinó:

> Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional.

Como se puede colegir de la simple comparación de estas normas, entre la primera versión de *habeas data*, recogida en las reformas a la Constitución de 1996, y la segunda, constante en la Constitución de 1998, únicamente existen dos diferencias:

a) *Eliminación de la referencia al juez competente para solicitar la actualización, rectificación, eliminación o anulación de los datos personales*. En el año 1996 la norma hacía referencia a que podía solicitarse ante el funcionario o ante el juez competente la actualización, rectificación, eliminación o anulación de aquella información que le perjudique. Para el año 1998, los titulares de un derecho

transgredido ya no podían exigir los derechos ARCO, con los que se materializa el *habeas data* ante el juez competente, sino que debían hacerlo ante el funcionario respectivo.

En resolución No. 0070-2003-HD[383] se señaló que el artículo 37 de la Ley del Control Constitucional se encontraba vigente, y no había sido declarado inconstitucional ni se habían suspendido sus efectos. Es decir que la norma que disponía que "La acción de hábeas data debía interponerse ante cualquier juez o tribunal de primera instancia del domicilio del poseedor de la información o datos requeridos" se encontraba vigente. Por tanto, aunque en la norma constitucional desaparecía la referencia al juez competente, sin embargo, en la práctica seguían siendo competentes los referidos jueces y tribunales para conocer y resolver la susodicha acción. Porque, según el Tribunal Constitucional:

> [...] tratándose de una garantía constitucional, quitar la competencia para su conocimiento a los jueces, sin que exista regulación alguna aparte de la norma constitucional, que establezca el procedimiento para que el «funcionario respectivo» (en caso de que no fuera un juez de lo civil), tramite la acción, resultaría que ni siquiera se contaría con una contestación negativa por escrito y sin ella el Tribunal Constitucional no podría resolver la apelación en virtud de lo dispuesto por el número 3 del artículo 276 de la Constitución, dejando a las personas en total indefensión".

Asimismo, las Salas del entonces Tribunal Constitucional eran competentes para conocer y resolver los recursos de *habeas data* respecto de las sentencias dictadas por Cortes Provinciales, de conformidad con lo que disponía el artículo 276 número 3 de la Constitución Política del Estado de 1998, en concordancia con el artículo 12 numeral 3, y artículo 62 de la Ley del Control Constitucional vigente a la época.

b) *Establecimiento de un procedimiento especial para acceder a datos personales que consten en archivos relacionados con la defensa nacional*. Se supera la idea de que el Estado deba tener secretos y, en consecuencia, se facilita la obtención de datos personales, incluso de aquellos que constan en archivos considerados de defensa nacional, claro está, mediante un procedimiento específicamente señalado por la ley. Adicionalmente, se sustituye la frase "seguridad nacional" por el de "defensa nacional" para especificar los ámbitos de aplicación de la confidencialidad, puesto que el primero se refiere a una visión Estado-céntrica de precautelar agresiones de Estados externos, mientras que defensa nacional se entiende como la operativización de esta protección del Estado frente a otros Estados externos que amenacen su soberanía; es decir, la organización logística y humana operativa de la seguridad nacional.

Para regular las garantías constitucionales introducidas en el año 1996, entre ellas el *habeas data*, en el año 1997 se dictó la Ley de Control Constitucional, que creó un capítulo específico titulado Del *habeas data*, el cual comprende los artículos del 34 al 45.

Asimismo, se mencionaba al *habeas data* en otras leyes: Ley Orgánica de la Defensoría del Pueblo,[384] la Ley Orgánica de Transparencia y Acceso a la Información Pública,[385] Ley

[383] TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0070-2003-HD].
[384] CONGRESO NACIONAL DEL ECUADOR, *Ley Orgánica de la Defensoría del Pueblo, Ley 1*, en RO, No. 7 (20 de febrero de 1997), *Lexis Ecuador*. ‹www.silec.com.ec›. Consulta: 22 de noviembre de 2017: "Artículo 2.-

Orgánica de Donación y Trasplante de órganos, tejidos y células,[386] etc., todas vigentes hasta la presente fecha.

Tanto en la Codificación de la Constitución de 1996 como en la Constitución de 1998, el *habeas data* tenía como fundamento el respeto al derecho a la intimidad; la idea de un derecho propio como el derecho a la protección de datos personales era todavía lejana.

Respecto de esta aseveración, el autor ecuatoriano Monseñor Larrea Holguín sostiene:

> Así como el Hábeas corpus tiene por finalidad garantizar la libertad, el Habeas data se dirige a proteger la honra y la intimidad de las personas. Los derechos sustantivos correspondientes están formulados fundamentalmente en el numeral 8 del artículo 23 de la Constitución: «el derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona.» [...] El habeas data es una garantía moderna, poco difundida todavía, pero que ya figura en algunas Constituciones como las de Colombia y de Perú, que inspiraron el proyecto de la Comisión de reformas de 1994, el cual ha sido aprobado por el Congreso y recogido en la Codificación de 1998. El texto de la Carta se refiere a varios aspectos del derecho: la información sobre los datos, la actualización, reforma de los mismos, su eliminación y la eventual indemnización por el perjuicio causado ilegítimamente.[387]

De lo anteriormente señalado, se puede colegir que la Constitución ecuatoriana de 1998 regulaba la protección de datos como lo hacía la mayoría de las latinoamericanas, esto es atada al derecho a la intimidad y mediante la garantía constitucional del *habeas data*. Aunque, conforme señalaba la mayoría de Constituciones de aquella época, entre las que constaba la ecuatoriana, al incluir el *habeas data* dentro del capítulo de las acciones procesales constitucionales, y por la forma en que se encuentra redactada en la norma, se concluye que este era, al mismo tiempo, una garantía constitucional y un derecho.

5.2 El *habeas data* entendido como derecho fundamental o como garantía constitucional

Del análisis evolutivo de la normativa constitucional, se puede colegir que, tanto en las reformas constitucionales de 1996 como en la Constitución de 1998, se concibió al *habeas*

Corresponde a la Defensoría del Pueblo: a) Promover o patrocinar los recursos de Habeas Corpus, *Habeas Data* y de Amparo de las personas que lo requieran".

[385] CONGRESO NACIONAL DEL ECUADOR, *Ley Orgánica de Transparencia y Acceso a la Información Pública, Ley 24*, en ROS, No. 337 (18 de mayo de 2004): "Artículo 8.- Promoción del Derecho de Acceso a la Información.- [...] Las universidades y demás instituciones del sistema educativo desarrollarán programas de actividades de conocimiento, difusión y promoción de estos derechos. Los centros de educación fiscal, municipal y en general todos los que conforman el sistema de educación básica, integrarán en sus currículos contenidos de promoción de los derechos ciudadanos a la información y comunicación, particularmente de los accesos a la información pública, hábeas data y amparo".

[386] CONGRESO NACIONAL DEL ECUADOR, *Ley Orgánica de Donación y Trasplante de Órganos, Tejidos y Células, Ley 0*, en RO, No. 398 (04 de marzo de 2011), *Lexis Ecuador*. ‹www.silec.com.ec›. Consulta: 22 de noviembre de 2017: "Artículo 11.- Prohibición de divulgación de información.- En ningún caso se facilitarán o divulgarán informaciones que permitan la identificación de la o el donante y/o de la o el receptor de los órganos, tejidos o células, salvo el caso de requerimiento de la función judicial, dentro del ámbito de su competencia, o mediante acción de *habeas data*, cuya audiencia tendrá carácter reservado. El funcionario que divulgue la información considerada como confidencial por la presente ley, será inmediatamente destituido sin perjuicio de las acciones que se puedan iniciar en su contra".

[387] J. LARREA HOLGUÍN, *Derecho constitucional ecuatoriano* (Quito: Corporación de Estudios y Publicaciones, 2000), 305.

data como una garantía constitucional la cual, al mismo tiempo, se constituía en un derecho fundamental dedicado a la protección de la intimidad informática. Aunque, en realidad, era una respuesta directa a las transgresiones producidas por el desarrollo de las tecnologías de la información y comunicación.

La Constitución de 1998 establecía mecanismos jurídicos que buscaban protección de los derechos, las libertades y su eficacia real. De tal forma que se consagraron dos formas de garantías. Aquellas referidas a los derechos como *habeas corpus, habeas data,* amparo, defensoría pública, y además aquellas relativas a las garantías básicas, destinadas a salvaguardar el debido proceso (véase el artículo 24 de la Constitución de 1998).

Según Monseñor Larrea Holguín:

> Se entiende por «garantías», en el campo del derecho público, todas las acciones u otros procedimientos prácticos que hacen efectivos los derechos. Los derechos son propiamente principios abstractos o declaraciones generales, que se protegen mediante acciones de diversa índole o por medio de recursos o procedimientos para remover lo que amenaza o afecta a los derechos, para reparar o indemnizar por el daño producido. A veces, sin embargo, en los mismos textos legales se confunden los términos y se usa el de garantías para expresar lo sustantivo, siendo así que propiamente de reservarse para lo adjetivo. La codificación de 1998 ha distinguido los derechos y las garantías de ellos, dedicando el Capítulo VI a las garantías, en tres secciones: 1º. De Hábeas Corpus, artículo 93); 2º. Del Habeas Data (artículo 94; 3ro Del Amparo (artículo 95; y, 4 De la Defensoría del Pueblo (artículo 96)".[388]

La mayoría de Constituciones, entre las que constaba la ecuatoriana de 1998,[389] incluyó el *habeas data* dentro del capítulo de las acciones procesales constitucionales; y al momento de establecer el texto señalan que el *habeas data* también es un derecho.

Entonces, el *habeas data* gozaba de esta doble calidad de constituirse una garantía constitucional y un derecho fundamental. Al respecto, debe señalarse la naturaleza jurídica de la garantía constitucional por la cual:

> [...] se encuentra destinada a la protección de derechos por disposición de la misma Constitución Nacional, se trata de una garantía. En atención a su carácter de acción judicial, reviste un obvio carácter procesal. Por tanto, se trata de una «garantía de carácter constitucional» correspondiente a la órbita del derecho procesal constitucional. Atento a su afinidad con el amparo y a las características de urgencia y expeditividad que ambos institutos comparte, se encuentra dentro del espectro de los denominados «procesos urgentes», los cuales «se tipifican cuando concurren situaciones que exigen una presta respuesta y solución jurisdiccional».[390]

De lo expuesto, el *habeas data* surge como una garantía que permite consagrar y proteger, al mismo tiempo, el derecho de los ciudadanos a fiscalizar sus datos y el mecanismo por el cual se logra su tutela efectiva, con lo cual se faculta la inmediata vigencia de un derecho que por su naturaleza debe ser solucionado rápidamente para evitar la prolongación de los daños que causa.

---

[388] Ibíd., 301.

[389] Ecuador, CONSTITUCIÓN POLÍTICA DEL ECUADOR [1998]. "Artículo 94.- Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito".

[390] G. PEYRANO, *Régimen legal de los datos personales y hábeas data*, 285.

Ahora bien, se debe aclarar que el *habeas data*

> [...] antes que una herramienta procesal, es un derecho disponible por el individuo que encuentra de esta forma una vía de acceso a información que le concierne, e inmediatamente, la potestad de resolver, por sí mismo con algunas pocas limitaciones, si quiere que esos datos se transmitan a otros, se conserven bajo reserva o confidencialidad, o se supriman por afectar la sensibilidad de la persona. Este conjunto de atributos suele nominarse como «derecho de autodeterminación informativa»… A su vez, el proceso garantista si bien sujeto al principio dispositivo, por sí mismo constituye un sistema cautelar o preventivo que no requiere de reglamentación para obrar en tal sentido, dentro del marco de posibilidades que el Derecho otorga (amparo, conocimiento, rectificación o cancelación).[391]

Para Oswaldo Gozaíni, el *hábeas data*, al ser una garantía de rango constitucional, necesita de un desarrollo legal, este es de índole complementario, pues lo significativo de un derecho-garantía es su aplicación directa y la posibilidad de la exigencia efectiva del derecho fundamental que consagra, ante un juez de primer nivel, quien solicita al funcionario o responsable particular que dispone de la información, el presentarla, explicar el uso que se está dando y el propósito de la entidad que tiene esa información; es decir, prescindir de acudir a entidades especializadas para iniciar reclamos administrativos, que eventualmente terminarán en la función judicial. Esta afirmación pudiera tener asidero si la única finalidad del *habeas data* fuera la de reaccionar ante las transgresiones producidas. Sin embargo, el derecho a la protección de datos personales tiene una faceta preventiva que no puede materializarse mediante esta acción constitucional, que solo puede ser interpuesta cuando el daño se ha producido.

5.3 Las garantías constitucionales en la Constitución de 2008

Históricamente, en Ecuador las garantías de los derechos constitucionales, pese a su reconocimiento expreso en la normativa, han sido objeto de sistemática e ilegítimas restricciones debido a la reducción de la noción de garantía exclusivamente a la esfera jurisdiccional o de la formalización o restricción formal de las garantías jurisdiccionales.[392]

Ante esa realidad, la Constitución de 2008 rompe el sistema preestablecido y concibe un sistema robustecido de protección de los derechos constitucionales. Por el cual, no se establece una gradación respecto a la protección de los derechos y libertades, sino que todos los derechos gozan de un régimen de protección jurídica reforzada que se logra por medio de garantías normativas o abstractas, jurisdiccionales o concretas e institucionales.[393] Se configuran entonces a las garantías desde su verdadera funcionalidad, de tal forma que se abandona la anterior perspectiva de que las garantías son en sí mismo derecho, para sostener en cambio que sin garantías prácticamente no hay derechos puesto que estarían ausentes los mecanismos de exigibilidad de una conducta u omisión que tales derechos implica. En palabras de Ferrajoli, la falta de normativa constituye una laguna o vacío normativo que debe ser solucionado.[394]

---

[391] O. GOZAÍNI, *Hábeas Data, protección de datos personales*, 107.
[392] A. GRIJALVA JIMÉNEZ, *Constitucionalismo en Ecuador*, 239.
[393] C. STORINI, "Las garantías constitucionales de los Derechos Fundamentales en la Constitución Ecuatoriana de 2008", en *La Nueva Constitución del Ecuador. Estado, derechos e instituciones* (Quito: Corporación Editora Nacional, 2009), 287-8.
[394] A. GRIJALVA JIMÉNEZ, *Constitucionalismo en Ecuador*.

El motivo por el cual se incluyen una mayor variedad de garantías constitucionales radica en que existen múltiples mecanismos, a más de las garantías jurisdiccionales, que obligan a las todas las instituciones y autoridades estatales a respetar y desarrollar los derechos humanos, no solamente los jueces.[395]

En consecuencia, se consagraron tres tipos de garantías:

a) **Las garantías normativas:** Son aquellas que buscan evitar que la actuación, con carácter general y abstracto, de los poderes públicos desconozcan, vulneren la eficacia o alcance de los derechos fundamentales, o menoscaben el contenido mínimo que la norma constitucional atribuye a dichos derechos. En virtud de lo cual, su finalidad primordial es evitar que las normas de rango inferior a la Constitución que desarrollan los derechos fundamentales despojen a éstas del contenido y de la eficacia que la Constitución le ha otorgado, sino ofrecer a cada ciudadano la posibilidad de reaccionar frente a las vulneraciones de sus propios derechos. "En el Estado de derecho esta reacción normalmente tiene lugar instando la actuación de los órganos judiciales, y por ello los instrumentos que la posibilitan se agrupan bajo la denominación de garantías jurisdiccionales o procesales específicas"[396]. Estas garantías conforme la clasificación doctrinaria se conocen como primarias porque obligan al Legislativo y al Ejecutivo en el ejercicio de su acción reguladora.

b) **Las garantías jurisdiccionales o procesales específicas:** Consisten en los instrumentos básicos para asegurar la efectividad de los derechos constitucionales. Por el cual, estas garantías son los medios procesales para exigir a los jueces, en cada caso en particular, aseguren de autoridades y particulares el respeto a los derechos constitucionales y obtener su restablecimiento o preservación.[397]

   En este sentido se ha pronunciado la jurisprudencia ecuatoriana cuando señala que:

   > La Constitución de la República en su condición de Norma Fundamental del Estado, consagra un amplio catálogo de derechos que determina las condiciones en las que se desarrolla y se establece el respeto de la dignidad de las personas. Las disposiciones contenidas en el catálogo de derechos constituye un elemento fundamental que tiene la persona para protegerse frente a la arbitrariedad de la autoridad o de las personas que ostentan alguna condición de poder. Las garantías jurisdiccionales constitucionales son las herramientas que el propio ordenamiento constitucional establece para poder concretizar y efectivizar el contenido de los derechos consagrados en la Carta Magna. Así, en este contexto, las garantías jurisdiccionales constituyen mecanismos judiciales mediante los cuales la justicia constitucional protege, cesa o impide la vulneración de los derechos. De allí que radica la importancia de estas herramientas para dotar de eficacia a los derechos y de esa forma, permitir la plena vigencia del Estado de derechos y justicia que implanta el marco constitucional. [398]

   Pertenecen a este grupo: la previsión de una acción de protección, acción de *habeas corpus*, acción de *habeas data*, acción por incumplimiento y acción de acceso a la

[395] Ibíd., 251.
[396] C. STORINI, "Las garantías constitucionales", 289.
[397] Ibíd.
[398] CORTE CONSTITUCIONAL, [Sentencia No. 00182-15-SEP-CC], en ROS, No. 596 (28 de septiembre de 2015).

información pública (artículo 88 y ss.). Posibilidad de promover una acción extraordinaria de protección ante la Corte Constitucional para la protección de los derechos reconocidos en la Constitución (artículo 94). Carácter obligatorio de la jurisprudencia de la Corte Constitucional en materia de garantías (artículo 436, núm. 6). Previsión de un procedimiento preferente y sumario para su protección jurisdiccional, de una reparación integral y de instrumentos para garantizar el efectivo cumplimiento de la sentencia o resolución (artículo 86).[399] Según la clasificación doctrinaria, a estas garantías se las denomina secundarias porque funcionan únicamente si las primarias han fallado y deben ser ejecutadas por jueces e incluyen sanciones o reparaciones.

c) **Las garantías de políticas, servicios públicos y participación ciudadana:** También denominada institucional, porque mediante mecanismos genéricos constituidos por acciones de gobierno y de la participación de la persona, comunidades, pueblos y nacionalidades se formulan, ejecutan, evalúan, y controlan políticas públicas y servicios públicos orientados a hacer efectivos todos los derechos y de su formulación y control ciudadano (artículo 85 de la CRE). No obstante, hay que entender como "garantía institucional aquel concepto relacionado con las instituciones que están garantizadas en la Constitución y, por tanto, aquellas otras garantías así definidas por algunos autores deben ser reconducidas, en función de su naturaleza".[400]

Hay que tener en cuenta, además, que todos los derechos gozan de otras garantías:

> 1. La protección que supone la existencia de una Corte Constitucional con capacidad para enjuiciar la conformidad de las leyes con los preceptos constitucionales relativos a derechos y libertades, por medio del control constitucional de las leyes. 2. La vinculación de todos los jueces y tribunales ordinarios a los derechos y garantías constitucionales, y, en especial, a realizar una interpretación de normas infra constitucionales favorable a los derechos constitucionales (artículo 11, núm. 5) y también a los funcionarios públicos. 3. La institución de la Defensoría Pública o Defensor Público y la Defensoría del Pueblo (artículo 191 y ss., 214 y ss.). 4. La institución de la Fiscalía General del Estado (artículo 194 y ss.). En suma, si se analiza la Constitución de Montecristi bajo el parámetro de la extensión de los mecanismos de protección de los derechos, podría afirmarse que representa un modelo ejemplar. No obstante, será necesario analizar si, y hasta qué punto, este modelo de garantías logrará ser realmente efectivo y, en su caso, cuáles podrían ser las interpretaciones del dictado constitucional que pueden favorecer dicha efectividad.[401]

Hay, sin embargo, un tercer género de garantías semijurisdiccionales o semipolíticas, consistentes en órganos de control independientes del Legislativo o del Ejecutivo, que tramitan denuncias o ejercen acciones para defender derechos constitucionales, pero no tienen poder de sanción; el ejemplo clásico es el del Defensor del Pueblo.

Conforme la clasificación antes citada, el *habeas data* es una garantía jurisdiccional, secundaria, pues procede solo una vez que la garantía primaria ha sido vulnerada; ya sea porque no existe normativa que proteja el derecho o porque, existiendo, se ha conculcado una

[399] Ibíd., 287-8.
[400] Ibíd., 289.
[401] Ibíd., 287-8.

norma constitucional o legal, que pretende garantizar la vigencia del derecho en un caso particular.

Con la finalidad de superar los problemas de la Constitución de 1998, la vigente plantea la desformalización del acceso a la garantía de *habeas data*. De este modo, en virtud del principio de universalización, permite que todas las personas puedan reclamar sus derechos, y en consecuencia, por aplicación todas las personas pueden ser parte legitimada de las garantías jurisdiccionales de la nueva Constitución. En el artículo 86 de la nueva Constitución se ratifica que "cualquier persona, grupo de personas, comunidad, pueblo o nacionalidad podrá proponer las acciones previstas en la Constitución". Mediante estos principios constitucionales se intenta pasar de una justicia constitucional altamente formalista, en la cual el acceso estaba fuertemente restringido, a una amplia posibilidad de actuación por parte de todos los ciudadanos.[402]

Asimismo, la nueva Constitución establece, en el artículo 86, varias disposiciones comunes que deben ser aplicadas tanto a garantías normativas, como a garantías jurisdiccionales e incluso de políticas y servicios públicos, incluidas las de participación ciudadana. Los principios comunes se refieren a los titulares, la competencia de los jueces que conocen estas acciones, los procedimientos pertinentes incluyendo medidas cautelares, audiencia, pruebas, sentencia y apelación, así como la ejecución de las sentencias, las sanciones por su incumplimiento y su eventual revisión por parte de la Corte Constitucional y la reparación integral, a lugar en una sentencia derivada de una acción constitucional cuando se ha violado un derecho establecido en la Carta Magna.[403]

Sin duda, la Constitución de 2008, contempla garantías como las normativas y jurisdiccionales, así como las relativas a las políticas, de servicios públicos y de participación ciudadana[404], que se interrelacionan para, en conjunto, completar y mejorar, el sistema de tutela de derechos.

En consecuencia, el *habeas data* no debe ser visto como la única posibilidad de protección de los derechos de las personas respecto de los derechos personalísimos de la honra, el buen nombre, la intimidad, la imagen, la propia voz, y la protección de datos personales sino que es necesario que se exija el cumplimiento de las otras garantías que constan descritas en la Constitución, esto es la garantía normativa que establece la obligatoriedad de la Asamblea Nacional de dictar la normativa que permita la tutela de estos derechos[405], así como de las

---

[402] A. GRIJALVA JIMÉNEZ, *Constitucionalismo en Ecuador*, 1041.

[403] Ibíd., 252.

[404] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR [2008], "Artículo 85: "La formulación, ejecución, evaluación y control de las políticas públicas y servicios públicos que garanticen los derechos reconocidos por la Constitución, se regularán de acuerdo con las siguientes disposiciones: 1. Las políticas públicas y la prestación de bienes y servicios públicos se orientarán a hacer efectivos el buen vivir y todos los derechos, y se formularán a partir del principio de solidaridad. 2. Sin perjuicio de la prevalencia del interés general sobre el interés particular, cuando los efectos de la ejecución de las políticas públicas o prestación de bienes o servicios públicos vulneren o amenacen con vulnerar derechos constitucionales, la política o prestación deberá reformularse o se adoptarán medidas alternativas que concilien los derechos en conflicto. 3. El Estado garantizará la distribución equitativa y solidaria del presupuesto para la ejecución de las políticas públicas y la prestación de bienes y servicios públicos. En la formulación, ejecución, evaluación y control de las políticas públicas y servicios públicos se garantizará la participación de las personas, comunidades, pueblos y nacionalidades".

[405] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR [2008], "Artículo 84.- La Asamblea Nacional y todo órgano con potestad normativa tendrá la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales, y los que sean necesarios para garantizar la dignidad del ser humano o de las comunidades, pueblos y nacionalidades. En ningún caso, la

otras garantías relativas a la formulación, ejecución, evaluación y control de las políticas públicas y de servicios públicos.

5.4 El *habeas data* en la Constitución de 2008

Como se ha visto, el *habeas data* existió desde 1996 y tenía una doble dimensión en la Constitución de 1998,[406] ya que era al mismo tiempo derecho y garantía. Incluso: "Gran parte de los derechos constitucionales son, en sí mismos, garantías de la realización de otros derechos, y que las mismas garantías deben considerarse derechos".[407]

El *habeas data*, al participar de esta doble virtualidad, paulatinamente había ganado independencia y autonomía, demostrando que por sí sola constituía tutela de un nuevo derecho fundamental conocido como: la libertad informática o autodeterminación informativa, por el cual el individuo tiene derecho al acceso y control de sus datos.

En tal sentido, la Constitución de 2008 consagró en el numeral 19 del artículo 66 de la CRE el derecho fundamental a la protección de datos personales en acápite distinto del derecho a la intimidad personal y familiar, ya que le otorgó contenido esencial distinto que justificó su inclusión en el catálogo de derechos y que fue analizado en líneas precedentes.

Ahora bien, respecto a lo que es de nuestro interés, la Constitución de 2008 perfecciona el sistema de tutela a través de la inclusión de nuevos tipos de garantías, y de normas comunes que regulan y efectivizan las garantías jurisdiccionales entre las que consta el *habeas data.*

Es pertinente realizar el análisis de la naturaleza jurídica de esta garantía jurisdiccional que conforme consta en el artículo 92 de la CRE textualmente señala:

> Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.

---

reforma de la Constitución, las leyes, otras normas jurídicas ni los actos del poder público atentarán contra los derechos que reconoce la Constitución".

[406] Ecuador, CONSTITUCIÓN POLÍTICA DEL ECUADOR DE 1998. Sección segunda, Del hábeas data: "Artículo 94.- Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional".

[407] C. STORINI, "Las garantías constitucionales", 287.

Para comprender las modificaciones y mejoras introducidas a la norma constitucional se realizó un análisis de la evolución normativa, comparando el texto que constaba en la Constitución de 1998 con el vigente de 2008. A continuación se señala las distintas variantes normativas y mejoras introducidas:

a) *Garantía Jurisdiccional:* En la nueva estructura constitucional la acción de *habeas data* está ubicada dentro del título III, Garantías Constitucionales, en el capítulo tercero de las garantías jurisdiccionales, en la cuarta sección denominada precisamente *Acción de hábeas data*. Es decir, a la luz de la Carta Magna vigente constituye una de las garantías jurisdiccionales y, junto con las garantías normativas y de políticas públicas, servicios públicos y participación ciudadana, conforman el actual sistema de garantías constitucionales.

b) *Legitimado activo:* El artículo 92 de la CRE aclara que toda persona "por sus propios derechos o como representante legitimado para el efecto" podrá ejercitar la garantía constitucional del *habeas data*. A diferencia de su versión anterior (1998), la norma vigente aclara que el legitimado activo de esta acción constitucional puede ser una persona como titular directa del derecho, así como su representante, en caso de carecer de capacidad de ejercicio. Incluso puede comparecer un representante legal de una persona jurídica, ya que como se analizó en líneas anteriores, la sentencia No. 001-2014-PJO-CC de carácter vinculante, dictada por la Corte Constitucional, reconoce que en Ecuador las personas jurídicas pueden ser titulares del derecho a la protección de datos.[408] A diferencia de lo establecido en la normativa europea, ya que ni el RGDP[409] ni la LOPD-GDD[410], otorgan este derecho a personas jurídicas pues expresamente lo limitan a personas físicas. La universalización de la titularidad, tanto del derecho fundamental como de la acción jurisdiccional, se configura también en el artículo 10 de la CRE que otorga personalidad jurídica, y por ende considera legitimados activos a personas, comunidades, pueblos, nacionalidades y colectivos.

c) *Derecho de información sobre la existencia de un fichero:* La Constitución vigente agrega un derecho que no constaba en la versión preliminar del artículo 92 de la CRE sujeta a análisis, que se refiere *a conocer de la existencia*; es decir, el *habeas data* no se limita al acceso, sino que desarrolla un nuevo contenido: el *derecho de información*, por el cual todas las personas tienen derecho a conocer de la existencia de un archivo, base de datos, información o documentos sobre sí mismo o sus bienes, ya sea que estos se encuentren en soporte digital o físico.

d) *Archivos de datos personales:* La norma vigente garantiza la protección no solo de documentos, bancos de datos e informes sobre sí misma o sobre sus bienes, sino que a diferencia de su predecesora incluye también a "los archivos de datos personales". Así

[408] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 001-2014-PJO-CC].

[409] Europa: REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PERSONALES: "Artículo 1 Objeto 1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos. 2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales".

[410] España: LEY ORGÁNICA 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales LOPD-GDD: "Artículo 1. Objeto de la ley. La presente ley orgánica tiene por objeto: (…) El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica".

pues, aparece el término *archivo*, comprendido como un "conjunto de datos almacenados en la memoria de una computadora que puede manejarse con una instrucción única. Conjunto ordenado de documentos que una persona, una sociedad, una institución, etc., producen en el ejercicio de sus funciones o actividades".[411] Se intenta con este término englobar toda la variedad de formas en las que se recoge datos personales; sin embargo, se deja por fuera a los datos sueltos que no cumplen con la condición de archivados. Además, se hace alusión expresa a que los datos susceptibles de protección son únicamente los personales, a diferencia de la norma anterior que no mencionaba esta específica naturaleza de los datos para que la garantía opere. En este sentido, es valiosa la aclaración de que la vigente garantía constitucional no protege cualquier tipo de dato, sino aquellos asociados a un titular identificado o identificable.

e) *Datos genéticos:* Asimismo, la norma vigente hace mención expresa a los datos genéticos, información sensible que debe ser protegida de forma especial por las repercusiones, no solo en la salud individual, sino incluso en el patrimonio biológico del Ecuador. Era voluntad de los asambleístas constituyentes la adición expresa de la protección de estos datos.[412]

f) *Soporte material y electrónico:* Se aclara que el *habeas data*, como acción, no solo protege los datos que constan en soporte electrónico, sino que se incluyen aquellos que consten en soporte material, dado que este derecho tiene como finalidad garantizar la dignidad humana no solo ante las agresiones tecnológicas, sino ante todas aquellas que pudieran, mediante la utilización de datos, causar una violación de derechos fundamentales.

g) *Derecho de información sobre la finalidad de una base de datos:* Se añade otro derecho que, de forma expresa, pasa a formar parte del actual contenido esencial del derecho a la protección de datos personales y de otros derechos conexos, los cuales se efectivizan mediante la acción constitucional del *habeas data* y que se refiere al derecho de información. Por el cual, el responsable de tratamiento debe informar al titular del dato, no solo sobre el derecho de acceso que ostenta sino sobre la finalidad o finalidades de un la recogida de datos, del tratamiento, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

h) *Difusión de la información por autorización del titular o la ley:* Otro de los derechos que se consagra en la nueva composición del texto constitucional del 2008 es aquel referido a que "Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley"; de este modo se establece un deber de abstención de difusión de la información, si previamente el responsable del fichero no cuenta con la autorización del titular del dato personal o es posible esta mencionada difusión por permitirlo expresamente la ley.

i) *Medidas de seguridad:* Asimismo, aparece en el texto de la Constitución vigente un principio propio de la protección de datos personales acerca de las medidas de seguridad. Sin embargo, llama la atención como el texto solo las propone como

[411] R. ASALE, "Diccionario de la lengua española - Edición del Tricentenario".
[412] ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 76], 12.

obligatorias para aquellos datos considerados sensibles y no para todos los datos personales. Esta postura normativa no permite el cumplimiento de aquellos principios que garantizan la efectiva vigencia del derecho a la protección de datos.

j) *Derecho ante la simple negativa de acceso por parte del responsable del fichero:* Al igual que en la versión de la Constitución de 1998, en el caso de que el funcionario no accediere a las peticiones de acceso, rectificación, cancelación o anulación de los datos, se puede acceder a un juez. Ahora bien, la diferencia radica en que en la versión anterior a la vigente este derecho de acudir ante juez competente solo operaba cuando los datos eran erróneos o afectaban ilegítimamente los derechos. Mientras que en la norma vigente para solicitar al juez su intervención, basta la simple negativa del administrador del archivo o base de datos, sin importar si el dato es erróneo o afecta sus derechos. En suma, se convierte en una aplicación del derecho a la libre autodeterminación informativa, por la cual cada persona puede decidir sobre qué datos entrega a determinada persona, en qué contextos, con qué finalidades y consecuencias bajo su propio criterio y voluntad.

   No obstante, pese a esa redacción constitucional que manifiestamente pretende el respeto a la autodeterminación informativa, nuevamente aparece el texto condicionante de la Constitución de 1998, pero ahora recogido en el artículo 50 de la Ley Orgánica de Jurisdicción y Control Constitucional. De tal forma que, volvemos al sistema anterior de protección, pues señala que el ámbito en el cual se podrá interponer la acción de *habeas data*, está previsto únicamente para los casos de negativa de acceso; de negativa en la actualización, rectificación, eliminación o anulación, cuando los datos fueren erróneos o afecten sus derechos; o cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente.

   Ahora bien, esta evidente limitación legal contraría uno de los principios de ejercicio de los derechos que consta en el artículo 11 de la CRE, el cual determina que ninguna norma jurídica puede restringir el contenido de las garantías constitucionales. Tanto más que, de la simple comparación entre las Constituciones de 1998 y la de 2008, se puede colegir que la eliminación de estas condiciones tiende a ampliar la garantía de derechos.

   Adicionalmente, el numeral 5 de la CRE establece que, en materia de garantías constitucionales, las servidoras y servidores públicos, administrativos o judiciales, deberán aplicar la norma y la interpretación que más favorezcan su efectiva vigencia. De tal forma que, las autoridades no podrían argumentar que deben cumplirse estas condicionantes para que proceda el *habeas data*. Porque a través de esta garantía no solo se protege el derecho a la protección de datos personales sino el derecho a la intimidad, el honor, la imagen y la voz e incluso la rectificación en medios de comunicación, como lo ha señalado la jurisprudencia[413], por lo que estos supuestos no serían aplicables necesariamente. Ya que, por ejemplo, en el caso de cualquiera de los derechos señalados, no se requiere que el dato difundido este equivocado o haya causado daño, o demostrar previamente se ha usado la información

[413] Ibíd., [Sentencia No. 0070-2003-HD], en ROS, No. 271 (11 de febrero de 2004); [Sentencia No. 0074-2004-HD], en RO, No. 417 (9 de septiembre de 2004); [Sentencia No. 0003-2008-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0020-2008-HD], en ROS 137 (4 de agosto de 2009); [Sentencia No. 0022-2008-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0038-2008-HD], en ROS, No. 133 (10 de julio de 2009).

y que esta ha violado un derecho constitucional para que el *habeas data* prospere. Este es el caso del derecho a la intimidad, cuya simple difusión del dato íntimo, sea correcto o no; haya o no causado un daño; se haya usado o no para violar un derecho (pues este simplemente puede estar potencialmente amenazado sin aun ser violentado), habilita interponer la garantía jurisdiccional de *habeas* data, por la sola voluntad de quien es el titular del dato.

Solo con una interpretación abierta, que no imponga limitantes a la procedencia, se viabiliza la vigencia efectiva de todos los derechos tutelados con el *habeas data*, más aún el derecho a la autodeterminación informativa, contenido esencial del derecho a la protección de datos personales. Es el titular, bajo su simple voluntad, el que autoriza o no el tratamiento de datos personales a un responsable y en consecuencia puede revocar ese consentimiento sin necesidad de que los datos sean incorrectos o dañinos.

k) *Solicitar indemnización:* En la versión de la Constitución de 1998 se mencionaba que el afectado podía demandar indemnización por la falta de atención del funcionario que le causare perjuicio, respecto de su solicitud de actualización, rectificación, eliminación o anulación, cuando los datos personales fueren erróneos o afectaren ilegítimamente sus derechos. El nuevo texto constitucional amplía el rango de cobertura por cuanto establece de forma abierta que la "persona afectada podrá demandar por los perjuicios ocasionados", cualquiera sea la naturaleza de estos; sin embargo, durante los debates constituyentes esta claridad no estuvo manifiesta. En varias intervenciones se argumentaba la necesidad de la existencia de un dato erróneo o de una transgresión o un daño ilegítimo a un derecho constitucional para que el *habeas data* opere.[414] La apertura de la norma tiene su razón de ser en la medida en que los perjuicios sufridos por un titular no solo pueden provenir de estas dos únicas fuentes, sino de un daño o perjuicio causado por el incumplimiento de cualquiera de las obligaciones de los titulares de un fichero o de los principios que regulan la protección de datos personales.

l) *Datos relacionados con defensa nacional:* Se elimina la frase: "La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional". La vigente Constitución elimina la concepción de defensa nacional para sustituirla por un concepto más amplio denominado seguridad integral,[415] el cual consta en el artículo 393 de la CRE; pero en ninguna parte del texto constitucional realiza alusión alguna a la forma en la que deberá accederse a este tipo de datos, por lo que se entiende que deberá utilizarse de forma general la garantía jurisdiccional de *habeas data*, teniendo como límite lo señalado en la Ley de Seguridad Pública del Estado, que clasifica a la información producto resultante de las investigaciones o actividades que realizan los organismos

[414] Ibíd., 45.

[415] La seguridad integral supera la visión estado-céntrica por la cual se protegía al Estado de agresiones externas o al Gobierno, su territorio y soberanía, para garantizar su supervivencia, ya que existen otros grupos no estatales que pueden afectar a la seguridad de una sociedad o que le procuran amenazas, como por ejemplo el terrorismo. Surge el concepto de seguridad integral, ya no solo del Estado como objeto de referencia, ni tampoco solo del ser humano (antropocéntrico), sino incluso del medioambiente, desde una visión biocéntrica de protección, por ejemplo de la soberanía alimentaria, recursos no renovables, tierras cultivables. Los actores en este entorno, ya no son únicamente las Fuerzas Armadas como protectoras de agresiones externas o la protección del orden público por intermedio de la Policía Nacional, sino que se articula un sistema integral que incluye servicios de emergencia como ECU 911, bomberos, defensa civil, entre otros.

de seguridad, en reservada, secreta y secretísima, y que, dependiendo de su naturaleza, pueden o no ser facilitadas al peticionario.[416]

m) *El Habeas data tutela varios derechos fundamentales:* Hasta antes de la vigencia de la Constitución de 2008, a nivel jurisprudencial, se consideraba al *habeas data* como la materialización del derecho a la intimidad. Actualmente, la garantía constitucional del *habeas data*, conforme su nuevo contenido, cobija no solo a la intimidad, sino al buen nombre, el honor, la imagen y la propia voz, así como al ahora autónomo e independiente derecho a la protección de datos personales. Esto debido a que todos estos derechos descansan en la necesidad de salvaguardar los datos de las personas para garantizar su dignidad.

> [...] Naturaleza: La acción de hábeas data es la garantía constitucional que le permite a la persona natural o jurídica, acceder a la información que sobre sí misma reposa en un registro o banco de datos de carácter público o privado, a fin de conocer el contenido de la misma y de ser el caso, exigir su actualización, rectificación, eliminación o anulación cuando aquella información le causan algún tipo de perjuicio, a efectos de salvaguardar su derecho a la intimidad personal y familiar. Contenido: La acción constitucional de hábeas data, protegerá el derecho a la intimidad, la honra, la integridad psicológica de la persona, puesto que no toda la información relativa a estos tiene el carácter de pública y por tanto de divulgable en forma libre. En efecto, existen asuntos relativos a su familia, sus creencias religiosas y espirituales, su filiación política, su orientación sexual, entre otras, que en caso de ser divulgadas de forma inadecuada e inoportuna podrían ocasionarle serios perjuicios en la esfera personal. Alcance: La acción constitucional de hábeas data tiene lineamientos específicos que deben ser observados por quien ejerce la legitimación activa de la misma, quien de forma especial, al redactar su pretensión deberá estructurar su pedido de conformidad con los parámetros establecidos para el efecto en la Constitución, en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional y en la jurisprudencia vinculante emitida por este Organismo sobre dicha acción lo cual coadyuvará, en primer lugar a que la acción en comento no se desnaturalice y en segundo lugar, a que la administración de justicia constitucional sea más ágil y eficaz para el fin que se persigue…".[417]

La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (LOGCC) desarrolló en el Capítulo VI esta acción constitucional en el título *Acción de hábeas data*. El artículo 49

[416] ASAMBLEA NACIONAL DEL ECUADOR, [Ley de Seguridad Pública y del Estado. Ley 0, ROS, No. 35 (28 de septiembre de 2009)]: "Artículo 19.- De la clasificación de la información de los organismos de seguridad.- La Secretaría Nacional de Inteligencia y los organismos de seguridad podrán clasificar la información resultante de las investigaciones o actividades que realicen, mediante resolución motivada de la máxima autoridad de la entidad respectiva. La información y documentación se clasificará como reservada, secreta y secretísima. El reglamento a la ley determinará los fundamentos para la clasificación, reclasificación y desclasificación y los niveles de acceso exclusivos a la información clasificada. Toda información clasificada como reservada y secreta será de libre acceso luego de transcurridos cinco y diez años, respectivamente; y si es secretísima luego de transcurridos quince años. La información clasificada como secretísima será desclasificada o reclasificada por el Ministerio de Coordinación de Seguridad o quien haga sus veces. De no existir reclasificación, se desclasificará automáticamente una vez cumplido el plazo previsto de quince (15) años. En ejercicio de los derechos y garantías individuales los ciudadanos podrán demandar ante la Corte Constitucional la desclasificación de la información en el evento de que existan graves presunciones de violaciones a los derechos humanos o cometimiento de actos ilegales".

[417] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 182-15-SEP-CC]. CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No.182-15-SEP-CC], ROS No. 596, 28 de septiembre de 2015).

de la mencionada ley repite de forma idéntica la norma constitucional, pero adiciona los siguientes elementos:

a) *Datos que deben permanecer en archivos públicos:* No podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos. De tal forma que se establece un límite a uno de los contenidos de las facultades del derecho a la protección de datos, pues por medio de la ley se establecen aquellos archivos que, además de recoger datos personales, deben ser públicos en garantía del bien común.

b) *Derecho de rectificación en medios de comunicación:* El penúltimo inciso del citado artículo 59 de la LOGCC señala que "las presentes disposiciones son aplicables a los casos de rectificación a que están obligados los medios de comunicación, de conformidad con la Constitución". En otras palabras, se realiza una extensión al alcance del *habeas data*, dado que no solo abarcaría el derecho a la protección de datos personales, intimidad, honor, buen nombre, imagen y voz, sino que se incluiría entre sus derechos tutelados, el derecho de rectificación en medios de comunicación social que consta en el numeral 7 del artículo 66 de la CRE.[418] Toda vez que, en estos casos, el derecho de rectificación no solo sería del dato en el archivo o base de datos al que se pertenezca, sino que como medida de reparación por el abusivo ejercicio del derecho a la libertad de expresión deberá efectuarse una rectificación, réplica o respuesta, en forma inmediata, obligatoria y gratuita, en el mismo espacio u horario en el que se transmitió la información que causó el perjuicio.

a) *Reparación integral:* Si bien el artículo 86 de la CRE establece, como disposición común a las garantías jurisdiccionales entre las que consta el *habeas data*, la obligación del juez de resolver la causa ordenando la reparación integral, es la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional la que establece el concepto de reparación integral, el cual incluirá todas las obligaciones materiales e inmateriales que el juez determine para hacer efectiva dicha reparación. Dicho de otro modo, el *habeas data* no se limita a un derecho indemnizatorio compensatorio de carácter económico, sino que faculta a solicitar todas aquellas acciones que permitan volver al estado anterior como si el daño no se hubiese producido jamás.

5.5 Clasificación del *habeas data*

A lo largo de este estudio por la doctrina, las diversas constituciones que ha tenido el Ecuador y su relación con la normativa vigente, esto es del análisis del artículo 92 de la Constitución, se puede colegir los tipos de *habeas data* reconocidos en el país:

a) *Habeas data informativo*, entendido como aquel que solo procura recabar la información necesaria para simplemente localizarla, conocer su finalidad, exigir la exhibición de los datos que se encuentran almacenados, saber quién otorgó los datos que constan en los ficheros, para con ello verificar si su recolección fue legal. Conforme consta en la jurisprudencia ecuatoriana, tiene la finalidad de "recabar

[418] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR DE 2008. "Artículo 66.- Se reconoce y garantizará a las personas: [...] 7. El derecho de toda persona agraviada por informaciones sin pruebas o inexactas, emitidas por medios de comunicación social, a la correspondiente rectificación, réplica o respuesta, en forma inmediata, obligatoria y gratuita, en el mismo espacio u horario".

información acerca del qué, quién, cómo y para qué se obtuvo la información considerada personal"[419].

b) *Habeas data aditivo o actualizador*, por el cual el ciudadano tiene derecho a "exigir agregar más datos sobre aquellos que figuren en el registro respectivo, buscando actualizarlo o modificarlo según sea el caso"[420].

c) *Habeas data rectificador o correctivo*, por el cual la persona tiene derecho a exigir la rectificación de sus datos cuando estos fueran erróneos o incompletos. Conforme nuestra jurisprudencia, "resuelve rectificar la información falsa, inexacta o imprecisa de un banco de datos"[421].

d) *Habeas data exclutorio o cancelatorio*, cuando el ciudadano manifiesta su voluntad de excluir los datos, sobre todo, cuando se trata de datos sensibles.

e) *Habeas data de reserva, en aplicación del* derecho de confidencialidad. Persigue asegurar que la información recabada sea entregada única y exclusivamente a quien tenga autorización para ello.

f) *Habeas data indemnizatorio*, que permite exigir al juez una indemnización cuando el funcionario no ha cumplido con la actualización, rectificación, eliminación o anulación de los datos. Se recalca que Ecuador es el único país que ha elevado a rango constitucional la indemnización; el resto de países suele incluirlos a nivel legal.

g) *Habeas data reparatorio*, reconocido en el numeral 3 del artículo 86 de la CRE y concordante con el artículo 18, el cual señala en las disposiciones comunes aplicables a todas las garantías constitucionales, entre las que se incluye al *habeas data*. La mencionada norma, en su parte pertinente, señala: "La jueza o juez resolverá la causa mediante sentencia, y en caso de constatarse la vulneración de derechos, deberá declararla, ordenar la reparación integral materia e inmaterial y especificar e individualizar las obligaciones, positivas y negativas, a cargo del destinatario de la decisión judicial, y las circunstancias en que deban cumplirse". En el mismo sentido, la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (LOGJCC) establece en el artículo 49 lo siguiente: "El concepto de reparación integral incluirá todas las obligaciones materiales e inmateriales que el juez determine para hacer efectiva dicha reparación". En conclusión, Ecuador es el primer país en reconocer un nuevo tipo de *habeas data* que supera la visión tradicional de carácter económico, y que permite solicitar una indemnización que incluya elementos inmateriales que propicie restituir el daño causado a un Estado, lo más cercano a considerar que este no se ha producido.

   Además, con respecto a esta clase de *habeas data*, se puede señalar que, como la norma exige la existencia de un daño a un derecho fundamental del afectado, esto es a la intimidad, honor, identidad, imagen, etc., el *habeas data* reparador opera solo si el funcionario que posee los ficheros no ha procedido a la actualización, rectificación,

[419] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 001-2014-PJO-CC].
[420] Ibíd.
[421] Ibíd.

eliminación o anulación de los datos cuando estos son erróneos o afectaren ilegítimamente sus derechos. Esto no ocurre con el derecho a la autodeterminación informativa para el cual la simple limitación a la libertad informativa de un titular de los datos es suficiente, pues es a este al que le corresponde decidir sobre los datos existentes, si desea o no mantenerlos disponibles, sin la necesidad de probar que el uso de estos datos haya causado un daño o estos estén incompletos, incorrectos, etc. Esta última afirmación no es del todo cierta, en virtud del contenido del artículo 50 de la LOGJCC, el cual establece una limitación cuando señala que solo podrá interponer la acción de *habeas data* cuando se niega el acceso; cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos si estos fueren erróneos o afecten sus derechos; o cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente. En otros términos, deben cumplirse cualquiera de estas causas cuando el derecho a la autodeterminación informativa no necesita de ninguna de estas condiciones en virtud de ser una forma de ejercicio del derecho a la autoconstrucción social e individual de una persona.

5.6 Legitimaciones activa y pasiva

El artículo 92 de la Constitución, en concordancia con el artículo 49 de la Ley Orgánica de Garantías Jurisdicciones y Control Constitucional, determina como legitimado activo a *toda persona*. Coincide con esta afirmación, el artículo 86 de la CRE que establece las disposiciones generales aplicables a las garantías jurisdiccionales, entre las que consta el *habeas data*, ya que en el numeral 1 señala expresamente: "Cualquier persona, grupo de personas, comunidad, pueblo o nacionalidad podrá proponer las acciones previstas en la Constitución". De tal forma que, la legitimación activa del *habeas data* habilita de forma general a casi todos los titulares de derechos establecidos en el artículo 10 de la CRE, exceptuándose únicamente a la naturaleza.

Se aclara que esta persona puede ejercer la acción por sus propios derechos o como representante legitimado para el efecto. Este representante lo puede ser de la persona natural, dado que esta no pueda actuar por sí misma por carecer de capacidad de ejercicio, o a su vez, es representante de una persona jurídica, comunidades, pueblos, nacionalidades y colectivos, en virtud de la universalización del acceso al goce de los derechos consagrados en el artículo 10 de la Constitución.

La Corte Constitucional, en Sentencia No. 001-14-PO-CC, de 3 de julio de 2014, referente a la acción constitucional de *habeas data*, señala como regla de jurisprudencia vinculante lo siguiente:

> 4. La legitimación activa para la presentación de la acción de hábeas data requerirá que quien lo haga sea el titular del derecho a la protección de datos personales que se alegue vulnerada, o su representante legitimado para el efecto.
> 5. Para acreditar la representación de las personas jurídicas será suficiente la entrega del documento que la ley que regule la materia determine como suficiente para considerar iniciadas sus funciones como representante. El juez constitucional, una vez acreditada la representación, deberá tramitar la acción sin que medie excepción sobre el cumplimiento de los requisitos de ley respecto del documento entregado, lo que deberá ser dilucidado por los organismos competentes en sede ordinaria.

Se aclara expresamente que la legitimación activa del *habeas data* pertenece a toda persona, natural o jurídica, por sus propios derechos o como representante legitimado para el efecto, conforme el artículo 51 de la LOGJCC.

Conforme consta de la propia norma constitucional, artículo 92 de la Constitución y artículo 49 LOGJCC, acerca de la legitimación pasiva, esta corresponderá a la persona responsable de los bancos o archivos de datos personales, quien en caso de no facilitar el acceso o de incumplimiento de las solicitudes de acceso, rectificación, eliminación o anulación deberá responder de la reparación integral que dicte el juez de la causa.

Las normas citadas hacen alusión a que el responsable de un fichero puede ser un funcionario público o un empleado privado.

Ahora bien, conforme dispone el artículo 215 de la Constitución de 2008, la Defensoría del Pueblo tendrá como funciones la protección y tutela de los derechos de los habitantes del Ecuador y de los ecuatorianos que estén fuera del país, entre los cuales consta, evidentemente, el derecho a la protección de datos personales y derechos conexos. Pero además, será parte de sus atribuciones el patrocinio, de oficio o a petición de parte, de las acciones de protección, *habeas corpus*, acceso a la información pública, *habeas data*, incumplimiento, acción ciudadana y los reclamos por mala calidad o indebida prestación de los servicios públicos o privados. De lo que se colige que el Defensor del Pueblo será un legitimado activo, en defensa de los derechos de particulares domiciliados o no en Ecuador, de la acción de *habeas data*, materia de análisis.

5.7 Procedimiento constitucional: jurisdicción, competencia y fases procesales

Tal como se ha previsto en el ejercicio de este derecho, existe una etapa preprocesal que consiste en que el legitimado activo acuda ante al funcionario público o privado, responsable del fichero, quien puede satisfacer inmediata y directamente las facultades de acceso, rectificación, eliminación o anulación.

Se deberá interponer acción de *habeas data* ante la negativa justificada o no del responsable de facilitar el acceso o el ejercicio de los derechos ARCO.

Conforme señala la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional en el artículo 167, compete a las juezas y jueces de primer nivel para resolver, en primera instancia, la acción de *habeas data*.

Asimismo, el artículo 168 del mismo cuerpo legal determina como competentes a las Cortes Provinciales para conocer y resolver los recursos de apelación que se interpongan en contra de los autos y las sentencias de las juezas y jueces de instancia respecto de la acción de *habeas data*.

El artículo 87 de la Constitución señala las disposiciones comunes aplicables a todas las garantías constitucionales y determina que se podrán ordenar medidas cautelares conjuntas o independientes de las acciones constitucionales de protección de derechos, con el objeto de evitar o hacer cesar la violación o amenaza de violación de un derecho. Estas medidas cautelares pretenden prevenir un daño irreparable. Y a través de ella solicita que se permita el acceso a datos que sean indispensables de ser conocidos en el momento actual, que se

conserven datos que pudieran estar en riegos de destruirse, que se modifique o elimine una información que podría o está causando un daño irreparable a otro derecho fundamental.

> Las diferencias respecto al procedimiento prevista por la Constitución de 1998 son considerables: desaparecen todas la formalidades procedimentales, eliminándose, por ejemplo, la obligación de presentar la demanda por escrito, la necesidad del patrocinio de un abogado, así como la posibilidad de presentar una demanda oralmente y sin necesidad de conocer la norma que se considera vulnerada, siendo suficiente la exposición de los hechos ocurridos.[422]

El artículo 191 de la norma citada, señala que será competencia del Pleno de la Corte Constitucional resolver sobre las sentencias de unificación respecto de la acción de *habeas data*.

Ahora bien, dictada la sentencia de *habeas data* y puesta en conocimiento del particular que debe dar cumplimiento a su contenido, este no la cumple, el juez deberá emplear todos los medios que sean adecuados y pertinentes para la ejecución de la sentencia o del acuerdo reparatorio, incluso podrá disponer la intervención de la Policía Nacional si fuere necesario.

Para garantizar el cumplimiento, el juez podrá expedir autos para ejecutar integralmente la sentencia e incluso podrá evaluar el impacto de las medidas de reparación en las víctimas y sus familiares; y de ser necesario modificará las medidas. Es más, el juez podrá delegar el seguimiento del cumplimiento de la sentencia o acuerdo reparatorio a la Defensoría del Pueblo o a otra instancia estatal, nacional o local, de protección de derechos. Dicha entidad podrá deducir acciones que sean necesarias para cumplir con esta delegación. Finalmente, la Defensoría del Pueblo o la instancia delegada deberá informar periódicamente a la jueza o juez sobre el cumplimiento de la sentencia o acuerdo reparatorio. El caso se archivará solo cuando se haya ejecutado integralmente la sentencia o el acuerdo reparatorio, de conformidad con el artículo 21 de la LOGJCC.

6. Situación del sistema de precedentes jurisprudenciales en Ecuador

Se puede construir una línea de evolución jurisprudencial del derecho a la protección de datos personales y de la garantía jurisdiccional del *habeas data*, mediante el análisis de las resoluciones que sobre la materia se han dictado por parte de la Corte Constitucional desde 1996 al 2019.

La fecha inicial de esta línea jurisprudencial se establece en virtud de la introducción del *habeas data* en la Tercera Reforma y Codificación de la Constitución de 1978, realizada en el año 1996. Estas reformas son las más importantes desde el retorno a la democracia; puesto que fortalecen las atribuciones del Tribunal Constitucional, estableciendo garantías de los derechos como: el recurso de amparo, *habeas data* y la figura del Defensor del Pueblo,[423] pero además, declaran al Tribunal Constitucional como instancia final de decisión en materia

[422] C. STORINI, "Las garantías constitucionales", 307.
[423] Sección II, De las garantías de los derechos; ¶ II, De La Defensoría del Pueblo; ¶ III, Del *Habeas Data*; ¶ IV, Del Amparo. Constitución Política de 1978, Tercera Codificación (1996), en RO, No. 969 (18 de junio de 1996).

de control constitucional.[424] Es decir, las competencias y funciones de la Corte Constitucional han ido cambiando, asimismo los efectos jurídicos de las sentencias dictadas por el más alto tribunal constitucional del Ecuador.

Los efectos vinculantes de las resoluciones examinadas varían dependiendo de la vigencia de la normativa constitucional y legal. Desde 1996 todas las sentencias son meramente referenciales; dicho de otro modo, no tienen efecto *erga omnes* pero orientan el contenido de un derecho o garantía y de ahí su importancia. Posteriormente, con la aprobación de la Constitución del 2008, los jueces del Tribunal Constitucional dejan de ser tribunales de instancia constitucional para convertirse en jueces de precedentes jurisprudenciales de aplicación generalizada.

Tradicionalmente, la ley ha sido la única y preponderante fuente de derecho, en tanto que la jurisprudencia, además de solo tener efectos intrapartes, a lo sumo y solo de forma excepcional, era considerada fuente auxiliar de interpretación. En este sentido, no se contemplaba a la jurisprudencia como fuente del derecho[425] y por ende no se hizo referencia

[424] "En Ecuador el control constitucional de la ley y de otras normas jurídicas ha pasado por tres etapas históricas: 1) soberanía parlamentaria (1830-1945); 2) surgimiento y desarrollo del Tribunal Constitucional (1945-1996); 3) desafíos de institucionalización (1996 hasta el presente)". Ver A. GRIJALVA JIMÉNEZ, *Constitucionalismo en Ecuador*, 171.

[425] La afirmación de que la jurisprudencia como fuente de derecho no haya tenido cabida alguna en la normativa ecuatoriana puede no ser del todo exacta. Si bien, en la jurisdicción constitucional no existía referencia alguna; sin embargo, en la jurisdicción ordinaria había estado presente y se había desarrollado paulatinamente. Inicialmente, y desde los albores de la República, por parte de la entonces Corte Suprema de Justicia, que funcionaba como tribunal de tercera instancia. Sus decisiones se consideraban doctrina jurisprudencial, que pretendía únicamente iluminar o justificar fundadamente una decisión. A este tipo de jurisprudencia se la denominaba referencial, pues carecía de efecto vinculante para el sistema judicial.
A partir de la Segunda Reforma y Codificación de la Constitución de 1978 (1993), que establece a la Corte Suprema de Justicia como tribunal de casación y de la promulgación de Ley de Casación, publicada en RO, No. 192 (18 de mayo de 1993), y reformada en RO, No. 39 (8 de abril de 1997), cuyo objetivo es la unificación normativa, se reconocen los precedentes jurisprudenciales. El artículo 19 de la mencionada ley establecía: "Publicación y precedente.- [...] La triple reiteración de un fallo de casación constituye precedente jurisprudencial obligatorio y vinculante para la interpretación y aplicación de las leyes, excepto para la propia Corte Suprema". Es decir, aparece por primera vez la denominada *jurisprudencia vinculante* que es aquella que no atraviesa por un proceso de selección y aprobación por parte de ningún órgano sino que basta su identificación por parte de abogados y jueces para que pueda solicitarse su aplicación en el caso particular sometido a jurisdicción. Obliga por tanto a jueces de instancia pero no a su emisor. Este tipo de jurisprudencia se generó hasta la Constitución de 2008.

Asimismo, el artículo 197 de la Constitución de 1998 contempló la competencia del Pleno de la Corte Suprema de Justicia, para casos de fallos contradictorios sobre un mismo punto de derecho entre Salas de Casación, Tribunales Distritales o Cortes Superiores, que se dicte una norma dirimente con carácter de obligatoria mientras la ley no determine lo contrario.

Posteriormente, la Constitución del 2008 y el Código Orgánico de la Función Judicial establecen un sistema reglado y organizado de jurisprudencia, al cual se ha denominado sistema de precedentes jurisprudenciales. Al respecto, el numeral 2 del artículo 184 dice: "Serán funciones de la Corte Nacional de Justicia, además de las determinadas en la ley, las siguientes: [...] 2. Desarrollar el sistema de precedentes jurisprudenciales fundamentado en los fallos de triple reiteración". Por su parte, el Código Orgánico de la Función Judicial, publicado en el Registro Oficial número 544, de 9 de marzo del 2009, en el artículo 180.2 establece: "FUNCIONES.- Al Pleno de la Corte Nacional de Justicia le corresponde: [...] 2. Desarrollar el sistema de precedentes jurisprudenciales, fundamentado en los fallos de triple reiteración".

Son parte de este sistema, aquellos fallos de triple reiteración sobre un mismo punto de derecho, que remitidos al pleno de la Corte Nacional de Justicia son analizados para por omisión o por ratificación de criterio constituyan jurisprudencia obligatoria. Los efectos de esta jurisprudencia son *erga omnes* pues obliga a la

de ella en el texto constitucional de 1978, ni en sus reformas. El mayor avance de la época como se vio se centró en otorgarle nuevas competencias al Tribunal Constitucional de aquel entonces, en especial, referentes a conocer las resoluciones que denieguen los recursos garantizados en la Sección II, "De las garantías de los derechos"[426] y a los casos de consulta obligatoria o apelación previstos en el recurso de amparo, conforme el artículo 175, numeral 3, Tercera Codificación de la Constitución de 1978.

La Corte Constitucional deja de ser otra instancia de apelación de sentencias de tribunales inferiores con finalidades particulares, cuyos efectos jurídicos se limitaban a la reparación de

---

sociedad en general y a todos los jueces, incluidos los de la Corte Nacional, que por excepción podrán modificar el criterio jurisprudencial obligatorio siempre y cuando se sustenten las razones jurídicas del cambio y la sentencia sea aprobada de forma unánime por la Sala que la dicta; así lo menciona el artículo 185 de la CRE de 2008.

Ahora bien, conforme el artículo 4 de la resolución emitida por el Tribunal en Pleno de la Corte Nacional de Justicia, el 1 de abril del 2009, publicada en el Registro Oficial número 572, de 17 de abril del mismo año, señala: "la jurisprudencia obligatoria expedida con anterioridad a la vigencia de la Constitución de la República, se rige por la norma prevista en el inciso segundo del artículo 19 de la Ley de Casación, mientras que la nueva, por los artículos 185 de la Constitución y 182 del Código Orgánico de la Función Judicial".

Respecto de la jurisprudencia que conforma parte del sistema de precedentes jurisprudenciales vigente en Ecuador cabe señalar lo siguiente:

a) La jurisprudencia dictada con anterioridad a la Ley de Casación y que fuera emitida por la Corte Suprema de Justicia, actuando como tribunal de instancia, se conoce como *jurisprudencia referencial* y no es parte del sistema, sino únicamente permite determinar el histórico de una interpretación judicial. Asimismo, se conoce como jurisprudencia referencial aquella que permanece en el tiempo en espera de ser reiterada en tres ocasiones y que permiten la paulatina construcción de triples reiteraciones obligatorias o la identificación de fallos contradictorios, y que también es mera doctrina jurisprudencial que no vincula a juez alguno, pues no ha superado el proceso de selección y aprobación que la convierta en obligatoria; esto es, tres fallos reiterados.
b) Aquella triple reiteración que fuera reconocida e invocada por jueces y partes en procesos judiciales al amparo de la Ley de Casación, anterior a la Constitución de 2008 y que vinculaba a jueces de instancia pero no a la Corte Suprema, denominada *jurisprudencia vinculante*.
c) Asimismo, conforma parte del sistema de precedentes aquella jurisprudencia que solucionaba conflictos mediante la norma dirimente, denominada *jurisprudencia de unificación* y que fuera establecida en el artículo 197 en la Constitución de 1998.
d) La *jurisprudencia obligatoria*, que es aquella reconocida como parte de un proceso de selección y aprobación por parte del Pleno de la Corte Nacional de Justicia, de conformidad con el artículo 185 de la Constitución de 2008.
e) Finalmente, la jurisprudencia denominada *resoluciones con fuerza de ley*, que de conformidad con el artículo 15 de la Ley Orgánica de la Función Judicial, publicada en el Registro Oficial 636, de 11 de septiembre de 1974, y del ahora vigente numeral 6 del artículo 180 del Código Orgánico de la Función Judicial, publicado en Registro Oficial Suplemento No. 544, de lunes 9 de marzo del 2009, la Corte Suprema de Justicia en ejercicio de sus facultades cuasilegislativas, en caso de duda y obscuridad de la ley, dicta resoluciones de aplicación obligatoria hasta que la ley disponga lo contrario.

De lo analizado, en Ecuador antes de la Constitución de 2008 existía un incipiente sistema de jurisprudencia obligatoria como fuente de derecho, este estaba fuera de la jurisdicción constitucional y pretendía armonizar y homogeneizar la aplicación de la normativa en resoluciones propias de la jurisdicción ordinaria. Actualmente, y en virtud de la Constitución vigente, comparte junto con la jurisdicción constitucional la característica de ser fuente de derecho y permite afirmar que, en el actual orden normativo, la jurisprudencia es fuente oficial, directa y obligatoria de derecho en Ecuador.

[426] La Tercera Codificación introdujo la Sección II a continuación de la denominada *De los derechos de las personas*. En ella, por primera vez, se organizaron las garantías constitucionales de tal forma que el primer parágrafo se refería al *habeas corpus*; se introdujo por primera vez en Ecuador, en el segundo parágrafo a la Defensoría del Pueblo, y en el tercer parágrafo al *habeas data*.

derechos exclusivos de las partes intervinientes, tal como sucedía con los extintos Tribunales Constitucionales, al amparo de la Constitución Política de 1998. Con la nueva Constitución, pasa a convertirse en una Corte que entre uno de sus deberes principales está la generación de derecho objetivo, aunque si durante el proceso de desarrollo de jurisprudencia vinculante se identifican vulneraciones a derechos constitucionales está facultada a reparar las consecuencias de dicha vulneración.[427]

En consecuencia, en la Constitución Política de 1998 tampoco se estableció el efecto vinculante y de aplicación general de la jurisprudencia dictada por la Corte Constitucional; al contrario su efecto era meramente secundario, referencial o de conocimiento. Incluso la actual Corte Constitucional, respecto de sus predecesoras, ha señalado que los Tribunales Constitucionales de la época "dictaban una serie de fallos contradictorios sobre una misma materia, circunstancia que denotaba que características como certeza y seguridad jurídica se endilgaban única y exclusivamente al derecho legislado, esto es, a la ley en sentido formal".[428]

La Constitución de la República de 2008 marca un cambio radical. Se reconoce a la jurisprudencia como fuente de derecho, y por ende, la exclusividad de la ley en sentido formal desaparece, permitiendo que otras manifestaciones no provenientes de la Asamblea, ni del Estado en general, reúnan condiciones para generar derecho objetivo. Precisamente, la jurisprudencia dictada por la Corte Constitucional cumple estos requisitos y se convierte en fuente de derecho válida y obligatoria para Ecuador.

Este reconocimiento de la jurisprudencia constitucional como fuente de derecho es posible gracias a la incorporación en la normativa constitucional, artículo 436, numerales 1 y 6 de la Carta Fundamental, del principio *stare decisis*.[429] Por el cual, es deber de los jueces decidir de acuerdo con lo resuelto en el pasado y no contradecir lo decidido sin una razón poderosa o mandatoria debidamente motivada o fundamentada; a esto es a lo que se conoce como carácter o jurisprudencia vinculante constitucional.

---

[427] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0023-2008-HD], 8. Al respecto, Emilio Suárez Salazar, refiriéndose a la jurisprudencia vinculante y el sistema de selección y revisión señala que: "la Corte Constitucional a través de su jurisprudencia, ha distorsionado el diseño original de esta institución, abriendo la posibilidad de que a través de ella se reabra el caso y exista un pronunciamiento sobre el fondo del mismo, tutelando derechos constitucionales. Esta distorsión desnaturaliza el diseño original del sistema, volviéndolo también una garantía jurisdiccional. En el Ecuador se ha institucionalizado la posibilidad de discutir la violación de derechos de las sentencias o resoluciones de una garantía jurisdiccional de conocimiento de jueces ordinarios a través de la acción extraordinaria de protección, siendo este el mecanismo idóneo para hacerlo. Lo mencionado vuelve innecesaria e inclusive peligrosa la distorsión que la Corte ha dado al sistema de selección y revisión de sentencias a través de su jurisprudencia, pues de esta manera inclusive puede existir la posibilidad de que se dicten sentencias contradictorias". Ver E. E. SUÁREZ SALAZAR, "Distorsiones del sistema de selección y revisión de sentencias de la Corte Constitucional Ecuatoriana", (Quito: Universidad Andina Simón Bolívar, 2015), 87.

[428] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0023-2008-HD], 7.

[429] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, resolución sobre inconstitucionalidad de la afiliación obligatoria cámaras gremios colegios, RTG 38 – ROS, No. 336 (14 de mayo de 2008): "stare decisis, las magistraturas en principio deben someterse a sus propios fallos, pues en caso contrario se podría vulnerar el principio de seguridad jurídica; ese sometimiento, bajo ningún concepto, puede prolongarse indefinidamente; ya que no debemos olvidar que el Tribunal Constitucional está para resguardar la integridad de la Constitución, no para sostener sus propios fallos, peor para reiterar errores, lo cual, es doblemente censurable, o volver a incurrir en ellos conscientemente".

El numeral 6 del artículo 436 de la CRE establece como competencia de la Corte Constitucional la de expedir sentencias que constituyan "jurisprudencia vinculante respecto de las acciones de protección, de cumplimiento, hábeas corpus, hábeas data, acceso a la información pública y demás procesos constitucionales, así como los casos seleccionados por la Corte para su revisión". Se reconoce, entonces, la existencia de reglas o *ratio decidendi* que generan efectos vinculantes para jueces de inferior o de igual jerarquía respecto a derechos y garantías jurisdiccionales; es decir, desarrollan jurisprudencia vinculante con carácter *erga omnes*.[430]

Para tal efecto, el artículo 86, numeral 5, de la CRE determina que todas las sentencias ejecutoriadas respecto de garantías jurisdiccionales de protección de derechos, incluidas medidas cautelares, que hayan sido dictadas por tribunales de apelación, esto es Cortes Provinciales, sean remitidas a la Corte Constitucional; la cual por medio de sus Salas de Selección y Revisión determinan aquellas sentencias que pueden servir para: a) crear reglas o precedentes sobre un conflicto identificado; b) ratificar una regla legislativa preexistente; c) aplicación de la cláusula abierta, esto es "en determinados casos incorporar normas al bloque de constitucionalidad por medio de sus fallos, por ejemplo, cuando estos son capaces de desarrollar el contenido de los derechos constitucionales o incorporar derechos implícitos o nuevos, en virtud de la cláusula abierta, prevista en el artículo 11, numeral 7 de la Constitución de la República".[431] El sistema de precedentes se constituye mediante la selección de casos tipo y casos difíciles, realizada por la Corte Constitucional, la cual dicta sentencias que se constituyen como jurisprudencia constitucional obligatoria para los demás jueces, que resuelven garantías y que unifican la interpretación de derechos fundamentales en todo el sistema judicial.[432] Ahora bien, existen sentencias que aunque dictadas con posterioridad a 2008 son rezagos del sistema anterior, y en consecuencia no son parte del sistema de precedente jurisprudencial y su contenido no será de obligatoria aplicación.

En conclusión, se considera que a partir de la Constitución de 2008 en Ecuador aparece un sistema de precedentes jurisprudenciales de carácter obligatorio. Que tampoco es inmutable pues se ha previsto un mecanismo para, de forma fundamentada, propiciar un cambio de línea jurisprudencial.[433]

La jurisprudencia ecuatoriana ha variado en su conceptualización y efectos, desde una ausente y casi nula aceptación como fuente de derecho a una concreción como fuente formal del derecho ecuatoriano. Asimismo, de tener efectos limitados exclusivamente a las partes procesales a establecerse como norma de conducta general, es decir, con efecto *erga omnes.* Ahora que la competencia para sustanciar y resolver las garantías jurisdiccionales ordinarias pertenece a jueces de primera instancia, quienes presentan dificultades respecto de la comprensión, alcance y aplicación de las garantías constitucionales o su correspondiente

[430] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0023-2008-HD], 6.
[431] D. ZAMBRANO ÁLVAREZ, "Jurisprudencia vinculante y precedente constitucional", en *Apuntes de Derecho Procesal Constitucional* (Quito: Centro de Estudios y Difusión del Derecho Constitucional, 2011), 233.
[432] A. GRIJALVA JIMÉNEZ, *Constitucionalismo en Ecuador*, 252.
[433] ASAMBLEA NACIONAL DEL ECUADOR, *Ley Orgánica de Garantías y Control Constitucional*, Segundo Suplemento, RO, No. 52 (22 de octubre del 2009): "Artículo 2.- Principios de la justicia constitucional.- Además de los principios establecidos en la Constitución, se tendrán en cuenta los siguientes principios generales para resolver las causas que se sometan a su conocimiento: [...] 3. Obligatoriedad del precedente constitucional.- Los parámetros interpretativos de la Constitución fijados por la Corte Constitucional en los casos sometidos a su conocimiento tienen fuerza vinculante. La Corte podrá alejarse de sus precedentes de forma explícita y argumentada garantizando la progresividad de los derechos y la vigencia del estado constitucional de derechos y justicia".

repercusión negativa en el caso concreto. Jurisprudencia vinculante que obliga a jueces, y permite garantizar seguridad jurídica, economía procesal, predicción de las decisiones judiciales, uniforme aplicación de las leyes, prestigio de los jueces y tribunales,[434] y además satisfacción en general de las necesidades de justicia de los usuarios del sistema.

Mientras se desarrolla cada uno de los temas de la presente investigación, se analizará la fundamentación de las resoluciones dictadas por la Corte Constitucional para el Período de Transición de 2008-2012[435] y de la actual Corte Constitucional de Ecuador que no son vinculantes[436]. Resoluciones que orientan la configuración histórica y paulatina del contenido esencial del derecho a la protección de datos personales y la garantía del *habeas data* en Ecuador.

Asimismo, sobre esta temática, se estudiará el único precedente jurisprudencial obligatorio[437] existente hasta la fecha; la consulta de norma con efecto vinculante[438]; y, la única resolución con efecto *erga omnes, relativa a la* interpretación de tratados internacionales de derechos humanos.[439] Resoluciones que permiten la determinación ecuatoriana del contenido esencial del derecho a la protección de datos personales en el Ecuador y de su correspondiente garantía constitucional, el *habeas data*.

Para cumplir con ese objetivo se desarrolló una metodología por la cual se investigó, identificó y seleccionó información jurisprudencial pertinente, útil y relevante. Se organizaron y sistematizaron todas las resoluciones sobre procesos de *habeas data*, disponibles en distintas fuentes,[440] dictadas por la Corte Constitucional del Ecuador en el período señalado. Posteriormente, se elaboraron fichas de resumen para tabulación de datos y determinación de las corrientes jurisprudenciales desarrolladas. Se creó un tesauro de términos básicos para la sistematización de la información. Se estableció una línea de tiempo y se identificó y analizó las pocas sentencias vinculantes que son parte del sistema de precedentes jurisprudenciales. Finalmente, se elaboró una tabla que contiene los insumos y resultados de la investigación. Todos estos productos constan en el anexo 1 de este trabajo doctoral.

---

[434] L. MORAL SORIANO, *El precedente judicial* (Madrid: Ediciones Jurídicas y Sociales S.A., 2002), 129 citado por Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 068-10-SEP-CC], 7.

[435] Dictadas por la Corte Constitucional para el Período de Transición de 2008-2012 en cumplimiento de la disposición transitoria primera de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, que señala que las acciones constitucionales establecidas en la Constitución de 1998 que se encuentran pendientes de despacho en la Corte Constitucional "...continuarán sustanciándose de conformidad con la normatividad adjetiva vigente al momento de iniciar su trámite, debiendo armonizarse con la Constitución del 2008".

[436] Dictadas, por la actual Corte Constitucional de Ecuador, en cumplimiento de la disposición transitoria primera de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, es decir las pendientes de despacho; así como aquellas dictadas en virtud de las atribuciones constantes en el artículo 94 y en el numeral 9 del artículo 436 de la CRE.

[437] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 001-2014-PJO-CC].

[438] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 006-17-SCN-CC], en ROEC, No. 22 (05 de diciembre de 2017).

[439] CORTE CONSTITUCIONAL, [Sentencia No. 00182-15-SEP-CC].

[440] No es posible revisar exclusivamente las publicadas en el Registro Oficial, o en la página web de la institución porque existen varios años en los cuales la información es incompleta debido a varias situaciones sobre todo de carácter político, ya que existen períodos de ausencia o transición de autoridades.

6.1 Práctica judicial anterior a la vigencia de la Constitución de 2008 respecto de *habeas data:* Tesauro jurisprudencial

Conforme ha señalado la propia Corte Constitucional, el desarrollo de jurisprudencia constitucional vinculante en materia de garantías es competencia exclusiva de la Corte Constitucional.[441] El *habeas data* se introduce en la normativa en 1996, aunque en ese momento la jurisprudencia dictada no tenía fuerza obligatoria, resulta interesante realizar un análisis que permita establecer cuáles fueron los criterios normativos y doctrinales utilizados, incluso identificar la interpretación contradictoria o coincidente realizada por el anterior Tribunal Constitucional y si estos problemas jurídicos han sido superados o tratados por la vigente Corte Constitucional. Además, resulta útil "la función ejemplificativa, por la cual el argumento permite que un enunciado normativo se le atribuya el significado que le ha sido atribuido por alguien".[442] Por este motivo, a continuación se realizará el análisis de las sentencias dictadas por la Corte Constitucional en materia de *habeas data* antes de la vigencia de la Constitución de 2008.

Por cuanto, esas sentencias no eran consideradas jurisprudencia obligatoria no se utilizará la identificación de la *ratio decidendi* ni de *obiter dicta*. Si bien, estos criterios podrían extractarse del texto de las resoluciones, incluso con fines ilustrativos; sin embargo, no tendría valor pues no generan el efecto específico de esta división, o sea, la *ratio decidendi* no tendría efecto vinculante respecto del *obiter dicta*.

En este caso, el estudio será histórico y meramente explicativo mediante el análisis de los pronunciamientos del Tribunal Constitucional; se identificarán las reglas y subreglas que marcan el desarrollo jurisprudencial. En primer lugar, se determinará un tema o descriptor, que consiste en el concepto o término jurídico de indización (hacer índices), autorizado o preferido que representan un concepto que se distingue o diferencia de otros conceptos del derecho y que puede ser visualizado en forma de sustantivo o frase sustantiva. Puede ser simple o compuesto, según esté formado por una o varias palabras. Dentro de cada descriptor o término genérico puede haber otros descriptores o términos particulares. En segundo lugar, se estipulará el subtema o restrictor, que son palabras o frases sobre un tema o aspecto específico y funcionan como subtítulos que guían y restringen la búsqueda.

Para el procesamiento jurisprudencial se utilizó una ficha que además de permitir la generación de un tesauro con temas, descriptores, subtemas o restrictores, recogió información de identificación general de la sentencia como número de expediente, autoridad que dicta la sentencia, fecha y número de emisión de la sentencia, decisión de la resolución constitucional, Registro Oficial o Gaceta Constitucional donde ha sido publicada la resolución constitucional, entre otros.

Asimismo, se analizaron las sentencias dictadas por el Tribunal Constitucional (1996), Corte Constitucional (1998), Corte Constitucional para el Período de Transición (2008 a 2012) y aquellos casos rezagados resueltos de la Corte Constitucional (2013 hasta la actualidad); mediante la utilización de los criterios de extracción de información, sistematización y procesamiento de sentencias, manejados por la vigente Corte Constitucional; estos son:

---

[441] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0023-2008-HD], 6.

[442] G. TARELLO, L'interpretazionedellalegge (Milano: Gufrre, 1980), 372, citado por L. MORAL SORIANO, *El precedente judicial* (Madrid: Ediciones Jurídicas y Sociales S.A., 2002), citado a su vez por CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 068-10-SEP-CC], 7.

1. Hechos relevantes: Como se trata de una contrastación de la realidad versus la normativa aplicada por los tribunales, para resolver los casos planteados es indispensable una correcta identificación de los hechos que motivaron la solicitud de la acción de *habeas data*. En el análisis jurisprudencial se debe tener especial cuidado con la descripción precisa y clara de los hechos porque la aplicación e interpretación normativa están directamente condicionados a estos.
2. Considerandos sobre la valoración de los derechos.
3. Descripción breve de la sentencia emitida por los jueces que conocieron la causa o determinación de los problemas jurídicos identificados por la Corte Constitucional.
4. Argumentos sobre la relevancia constitucional.

El levantamiento completo de la presente investigación en su versión digital se encuentra adjunta en el Anexo 1.[443]

La forma de presentación del procesamiento jurisprudencial será por medio de un tesauro; es decir, de los principales temas o descriptores y subtemas o restrictores mediante los cuales se puede determinar los criterios utilizados en la práctica judicial constitucional de la época. Esto es, las diferentes peculiaridades de la aplicación del *habeas data* en el caso concreto, su alcance y contenido e incluso las posibles contradicciones existentes.

Los principales ámbitos de análisis son aquellos relativos a: a) la naturaleza jurídica del *habeas data*; b) los derechos a ser protegidos por parte del *habeas data*; y, b) los aspectos procesales de esta garantía constitucional en los cuales se desarrollarán temas y los respectivos subtemas. Dicho de otra manera, una red intrincada de interpretaciones judiciales que delineaban el contenido del derecho, aunque, lamentablemente, a la fecha solo constituyan mera referencia, o doctrina jurisprudencial, que si bien puede ser invocada por jueces y partes tienen la limitación de solo ser orientadora y no vinculante.

6.1.1 Naturaleza jurídica del *habeas data*

6.1.1.1 Garantía constitucional que protege varios derechos

En la sentencia No. 0070-2003-HD[444] se señala que el *habeas data* es una garantía constitucional que tiene por objeto proteger el acceso a la información personal, así como el derecho a la honra, a la buena reputación y a la intimidad personal y familiar, que son derechos personalísimos;[445] y, en consecuencia, el artículo 94 de la Constitución Política del Estado da derecho a toda persona a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito, y a solicitar la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. De esta aseveración realizada llama la atención que, incluso desde antes de la vigente Constitución de 2008, de que la garantía constitucional del *habeas data* no solo

[443] El anexo incluye el plan y cronograma de investigación, la matriz de procesamiento de jurisprudencia, la ficha de levantamiento de información, la base de datos que contiene todas las sentencias a texto completo analizadas y la base de datos con el total de la jurisprudencia procesada.
[444] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0070-2003-HD].
[445] Ibíd., [Sentencia No. 0070-2003-HD], en ROS, No. 271 (11 de febrero de 2004); [Sentencia No. 0074-2004-HD], en RO, No. 417 (9 de septiembre de 2004); [Sentencia No. 0003-2008-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0020-2008-HD], en ROS 137 (4 de agosto de 2009); [Sentencia No. 0022-2008-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0038-2008-HD], en ROS, No. 133 (10 de julio de 2009).

protegía el derecho a la intimidad personal y familiar,[446] sino que incluía otros derechos como la honra, la buena reputación e incluso menciona a la integridad moral de las personas,[447] todos ellos por su estrecha relación con la privacidad de las personas.

En similar sentido al anteriormente descrito, la sentencia No. 0007-2006-HD[448] señala que el *habeas data* es una garantía constitucional que tiene por objeto el derecho a la información y el honor, el buen nombre, la dignidad de la persona; es decir, reconoce el carácter plural de esta garantía que no protege un derecho, sino una multitud de derechos. Anotándose que la referencia a la dignidad de la persona como centro de protección permite determinar el carácter amplio e inclusivo de esta garantía constitucional que desde distintas perspectivas protege derechos fundamentales.

> De lo indicado en el considerando anterior, se desprende también, que la acción de hábeas data tiene dos presupuestos que la hacen procedente, y que deben operar en forma relacionada, tales son: Que la información en poder del requerido debe pertenecer al solicitante, y que se considere de manera fundada, que la información puede llegar a afectar el honor, la buena reputación, la intimidad o irrogar daño moral a la persona.[449]

Esta postura jurisprudencial se ha mantenido con el siguiente texto que consta en varias de las resoluciones del año 2008 que dice textualmente:

> El hábeas data es una garantía constitucional que tiene por objeto proteger el acceso a la información personal, así como el derecho a la honra, a la buena reputación y a la intimidad personal y familiar, en consecuencia es derecho de toda persona para acceder a los documentos, banco de datos o informes que sobre sí misma, o sus bienes consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellas y su propósito; de ello, se advierte que toda persona natural o jurídica está facultada para requerir del poseedor de la información, que haga relación a ella y que le sea entregada en los términos que establece la norma constitucional.[450]

Se ha superado la limitada visión de la protección del *habeas data* y se ha ampliado su contenido, no solo al derecho a la intimidad, sino a otros derechos fundamentales incluido el derecho a la protección de datos personales.

---

[446] Ibíd., [Sentencia No. 0068-08-CC], en ROS, No. 535 (26 de febrero de 2009); [Sentencia No. 0076-2008-HD], en ROS, No. 111 (25 de marzo de 2009).
[447] Ibíd., [Sentencia No. 0022-2004-HD], en RO, No. 353 (10 de junio de 2004).
[448] Ibíd., [Sentencia No. 0007-2006-HD].
[449] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR [Sentencia No. 0039-2008-HD], en ROS, No. 86 (5 de diciembre de 2008); [Sentencia No. 0053-2004-HD], en RO, No. 389 (de 30 de julio de 2004); [Sentencia No. 0019-2007-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0048-2007-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0003-2008-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0005-2008-HD], en ROS, No. 68 (05 de agosto de 2008); [Sentencia No. 0031-2008-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0038-2008-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0083-2008-HD], en ROS, No. 126 (9 de junio de 2009); [Sentencia No. 0001-2009-HD], en ROS, No. 111 (25 de marzo de 2009); [Sentencia No. 0004-09-HD], en ROS, No. 590 (14 de mayo de 2009).
[450] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR PARA EL PERIODO DE TRANSICIÓN, [Sentencia No. 0074-2008-HD], en ROS, No. 8 (4 de septiembre de 2009); [Sentencia No. 0039-2008-HD], en ROS, No. 86 (5 de diciembre de 2008); [Sentencia No. 0076-2008-HD], en ROS, No. 111 (25 de marzo de 2009); [Sentencia No. 0051-2008-HD], en ROS, No. 531, (18 de febrero de 2009); [Sentencia No. 0079-2008-HD], en ROS, No. 8 (4 de septiembre de 2009); [Sentencia No. 0003-2009-HD], en ROS, No. 122 (13 de mayo de 2009); Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR PARA EL PERÍODO DE TRANSICIÓN, [Sentencia No. 019-09-SEP-CC2], en ROS, No.018 (3 de septiembre de 2009).

6.1.1.2 No procede *habeas data* de documentos con carácter de reservados por razones de Seguridad Nacional

En el sentencia No. 010-HD-01-I.S. se niega el *habeas data* solicitado en contra del Presidente del Consejo de Generales de la Policía Nacional del Ecuador, por cuanto el Tribunal Constitucional sostiene que artículo 36 de la Ley de Control Constitucional dispone que:

> "No es aplicable el Hábeas Data cuando afecte al sigilo profesional; o cuando los documentos que se soliciten tengan el carácter de reservados por razones de Seguridad Nacional". Y que en este caso, el artículo 42 del Reglamento del Consejo de Generales de la Policía Nacional dispone que las actas, informes y más documentación existente en el Archivo del Consejo, tendrá el carácter de secreto o reservado.

Si bien, en las reformas constitucionales de 1996, bastaba con que la información sea catalogada como reservada como para que sea inadmisible el *habeas data*. Este uno de los temas modificados en la Constitución de 1998, ya que constaba expresamente el inciso final del artículo 94 que la ley establecerá un procedimiento especial para acceder a los datos personales que consten en archivos relacionados con la defensa nacional. En tal virtud, la norma invocada y aplicada por el Tribunal Constitución, esto es el artículo 36 de la Ley de Control Constitucional, no podía ser aplicada de forma descontextualizada sin respetar lo dispuesto por la entonces vigente norma constitucional, y por lo tanto, el *habeas data* no podría haberse negado de plano como consta en la mencionada sentencia.

6.1.1.3 No es finalidad del *habeas data* dar tranquilidad

En la normativa vigente a la época, al *habeas data* no le correspondía el contenido del derecho a la autodeterminación informativa, y en este contexto era necesario justificar las causas legítimas para solicitar el acceso a la información personal, por eso es que en la sentencia No. 0034-2006-HD, antes de la incorporación del derecho a la protección de datos en Ecuador, no era finalidad del *habeas data* dar tranquilidad al titular de los datos:

> Del contenido de la demanda se observa que la pretensión del accionante no es, en esencia, el acceso a la información en los términos que ha sido concebido el hábeas data como garantía constitucional, ya que, expresamente señala en su petición que el objetivo de ésta acción es obtener tranquilidad y seguridad respecto a que la indagación previa "no ha sido robada, desaparecida o perdida" y, además, de los antecedentes que ha señalado, se establece que la documentación requerida inicialmente al fiscal serviría para iniciar acciones legales en su contra.[451]

6.1.1.4 Diferencia entre acceso a la información y *habeas data*

Aunque resulta comprensible de la simple lectura de los artículos 91 y 92 de la CRE, la acción de acceso a la información pública difiere en esencia del *habeas data* debido a que hace referencia a datos de diferente naturaleza.

[451] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0034-2006-HD], en ROS, No. 371 (05 de octubre de 2006); [Sentencia No. 0048-2007-HD], en ROS, No. 133 (10 de julio de 2009).

El acceso a la información pública, hacer referencia a datos públicos, comprendidos como aquellos generados en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas, conforme señalan los artículos 18 numeral 2 de la CRE, 1 y 5 de la Ley orgánica de transparencia y acceso a la información pública.

El *habeas data* por su parte se aplica a información de las personas y por ende su ámbito son los datos personales, tanto si a través de ellos se afecta el derecho a la protección de datos personales, como otros derechos: intimidad, honra, imagen y voz o rectificación en medios públicos.

En la jurisprudencia que se relata a continuación, se hace referencia a que no se puede acceder a información pública a través de la garantía jurisdiccional del *habeas data*.

> Es evidente que la mayor parte de la información a la que solicitan acceso los actores se relacionan con hechos, circunstancias, procesos y actos ajenos a sus personas y sus bienes, respecto de los cuales no procede el hábeas data pues se trata de la gestión municipal en una determinada área urbanística a cuyo conocimiento puede acceder la ciudadanía en ejercicio del derecho a la información, como consecuencia de la transparencia y publicidad que reclama la actividad pública, pero no mediante acción de hábeas data que garantiza el acceso a la información que consta en las instituciones en torno a datos personales y patrimoniales de los ciudadanos.[452]

6.1.1.5 *Habeas data* no es un mecanismo constitucional supletorio de otros procedimientos

Debido al abuso en la interposición de esta garantía constitucional, se aclara que no puede ser utilizada para finalidades distintas a su naturaleza[453] y por ende no puede convertirse en "un mecanismo supletorio de procedimientos establecidos en el ordenamiento jurídico"[454]. Por lo que, no puede utilizarse en lugar de procedimientos propios de otras vías jurisdiccionales, es decir "no debe confundirse ni pretender ser utilizado paran reemplazar ningún tipo de procedimiento ordinario, sea civil o penal"[455].

---

[452] Ibíd., [Sentencia No. 0007-2006-HD], en ROS, No. 349 (5 de septiembre de 2006).

[453] "las garantías jurisdiccionales tienen que constituir mecanismos constitucionales idóneos para una protección eficaz e inmediata de los derechos consagrados en la Constitución de la República, de acuerdo a su naturaleza jurídica y finalidades específicas, de modo que, en atención a su objetivo principal, no sean propuestas de manera inapropiada". Ibíd., Sentencia No. 175-14-SEP-CC] en ROEC, No. 406 (30 de diciembre de 2014); [Sentencia No. 0002-14-HD] en ROEC, No. 2 (5 de junio de 2017)

[454] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0046-2002-HD], en ROS, No. 66 (22 de abril de 2003; [Sentencia No. 0044-2007-HD], en RO, No. 137 (4 de agosto de 2009); [Sentencia No. 0018-2001-LID], en ROS, No. 370 (17 de julio de 2001); [Sentencia No. 0031-2001-BID], en ROS, No. 393 (20 de agosto de 2001); [Sentencia No. 0048-2007-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0028-2008-HD], en ROS, No. 86 (5 diciembre de 2008); [Sentencia No. 0009-09-HD], en ROS, No. 1, (18 de agosto de 2009); [Sentencia No. 0001-12-HD], en ROS, No. 949 (8 de mayo de 2013), [Sentencia No. 0001-13-HD], en ROSEC, No. 2 (5 de junio de 2017).

[455] Ibíd., [Sentencia No. 0044-2007-HD], en RO, No. 137 (4 de agosto de 2009); [Sentencia No. 0018-2001-LID], en ROS, No. 370 (17 de julio de 2001); [Sentencia No. 0031-2001-BID], en ROS, No. 393 (20 de agosto de 2001); [Sentencia No. 0048-2007-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0028-2008-HD], en ROS, No. 86 (5 diciembre de 2008); [Sentencia No. 0009-09-HD], en ROS, No. 1, (18 de agosto de 2009); [Sentencia No. 0001-12-HD], en ROS, No. 949 (8 de mayo de 2013), [Sentencia No. 0001-13-HD], en ROSEC, No. 2 (5 de junio de 2017).

En el mismo sentido, la cita que consta a continuación:

> "el *habeas data* no es un mecanismo constitucional que busque reemplazar procedimientos y atribuciones establecidos en el ordenamiento legal. En esta línea, los recurrentes solicitan la exhibición de documentos de terceros que reposan en registros públicos, pretensión para la cual se han previsto mecanismos procesales en la justicia ordinaria.[456]

Asimismo, el *habeas data* tampoco puede ser usado para reemplazar otros medios de acceso de información general previstos en vía ordinaria y que en muchos casos está relacionado a la obtención de pruebas[457] para procesos judiciales:

> De la revisión de la jurisprudencia constitucional existente bajo la regulación de la Constitución Política de 1998, podemos ver que la Corte Constitucional al resolver los recursos de Hábeas Data fue clara en señalar que el recurso de Hábeas Data no podía, ni puede ser utilizado como un mecanismo para reemplazar otros medios para acceder a información general.[458]

6.1.1.6 Diferencia entre confesión judicial y *habeas data*

Una inadecuada aplicación de la garantía constitucional del *habeas data* es la de ser utilizada como mecanismo para obtener una confesión judicial, conforme consta de la jurisprudencia que se detalla a continuación:

> El pedido del accionante que consta de fojas 3 a 5 del expediente, no indica cuales documentos requiere, más bien realiza un pliego de preguntas a manera de Confesión Judicial, lo que nada tiene que ver con el Recurso de *Habeas Data*, que es un proceso que se inicia con el acceso a la información, permitiendo a quien accede analizarla y determinar si esa información es correcta o no y si debe o no ser divulgada; que continúa con el pedido de rectificación, eliminación o no divulgación y que concluye con la certificación de que se ha eliminado, corregido o no divulgado. Siendo evidente, que el acceso a tal información tiene como finalidad primigenia, la protección del honor, la buena reputación, en suma la intimidad, derecho elevado a rango constitucional, parte inherente a la dignidad humana.[459]

De lo descrito, es evidente que no se puede desnaturalizar al *habeas data* para solicitar que una persona realice una confesión judicial, ya que existen mecanismos procesales pertinentes para obtener este tipo de prueba. La obtención de información de una persona a través de un pliego de preguntas no es pertinente al *habeas data*, que tiene por finalidad acceder a datos recogidos en soportes físicos o digitales no en el fuero interno de las personas.

6.1.1.7 Diferencia entre exhibición de documentos de *habeas data*

La sentencia No. 046-2002-HD[460] aclara los objetivos de la acción de *habeas data* para distinguirla de la ordinaria de exhibición de documentos. Así, la acción constitucional permite el acceso a la información, se verifica su exactitud, uso, también se impide que se

[456] Ecuador, CORTE CONSTITUCIONAL, [Sentencia No. 1-17-HD], en ROEC No. 70 (29 de marzo de 2019)
[457] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0022-2008-HD], en ROS, No. 133 (10 de julio de 2009).
[458] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0001-15-11D], en ROEC, No. 70 (29 de marzo de 2019). [Sentencia No. 0002-14-HD] en ROEC, No. 2 (5 de junio de 2017)
[459] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0022-2008-HD], en ROS, No. 133 (10 de julio de 2009).
[460] Ibíd., [Sentencia No. 0033-2004-HD].

difunda si está errada, se cambia si es equivocada y se difunde la verdadera información entre aquellos a quienes el poseedor de ella la remitió o circuló; todo con el propósito de proteger o resguardar los derechos constitucionales subjetivos. En cambio, la de exhibición de documentos procede para fundamentar una demanda o contestarla, consecuentemente tiene un carácter probatorio para ser utilizado en un proceso civil como acto preparatorio o como diligencia sustanciada. En consecuencia, para determinar la acción correcta se debe contrastar los fundamentos de hecho y de derecho de la demanda de *habeas data* en cada caso presentado, pues el *habeas data* no puede convertirse en un mecanismo supletorio de procedimientos establecidos en el ordenamiento jurídico.

Conforme lo dictamina la Corte Constitucional, en la sentencia No. 0044-2007-HD, la acción de *habeas data* procede por el tipo de información que se solicita y su finalidad, conforme se analiza en el extracto de la sentencia transcrita a continuación:

> [...] En este sentido, se establece que la diferencia fundamental entre la exhibición de documentos y la acción de *habeas data* está dada por el tipo de información requerida y la finalidad perseguida con tal acción; para ello, debe tomarse en cuenta que no se trata de cualquier tipo de información, sino aquella relacionada con información personal, cuya divulgación cause perjuicio o viole su derecho a la intimidad, al honor y a la buena reputación, y que la finalidad es justamente conocer qué uso se está dando a esa información, para hacer efectiva la protección de sus derechos.[461]

La siguiente cita analiza la relevancia del tipo de información al que se quiere acceder a través del *habeas data*. Si se trata de aquella protegida a nivel constitucional o de la que amerita únicamente una protección infraconstitucional, para lo cual deberá determinarse si transgrede o no derechos constitucionales, al tenor de lo siguiente:

> Por tanto, si no se trata de información constitucionalmente relevante a la que el peticionario pretende acceder, el ordenamiento jurídico dispuso otro mecanismo en el nivel infraconstitucional que permite cumplir con este objetivo, denominado por el legislador como "acto preparatorio o exhibición de documentos", que encontraba su regulación normativa en el Código de Procedimiento Civil, normativa aplicable a la fecha de presentación de la demanda. Por lo dicho, la Corte Constitucional no desconoce de la existencia de un interés legítimo de los accionantes para acceder a la documentación solicitada, sin embargo, no se observa, de forma razonable, qué derecho constitucional se encuentra vulnerado o podría ser vulnerado en caso de que se prohíba la exhibición de los documentos.[462]

Asimismo, es fundamental distinguir el ámbito de su exigencia y aplicación por cuanto conforme consta en la Sentencia No. 0039-2008-HD:

> La diferencia esencial entre la exhibición de documentos como prueba o diligencia previa, y la acción de hábeas data, está dada por el ámbito en el que son exigibles. La primera es intrínsecamente una acción de legalidad, mientras que el hábeas data, doctrinaria y

[461] Ibíd., [Sentencia No. 0044-2007-HD], en RO, No. 137 (4 de agosto de 2009); [Sentencia No. 0018-2001-LID], en ROS, No. 370 (17 de julio de 2001); [Sentencia No. 0031-2001-BID], en ROS, No. 393 (20 de agosto de 2001); [Sentencia No. 0048-2007-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0028-2008-HD], en ROS, No. 86 (5 diciembre de 2008); [Sentencia No. 0009-09-HD], en ROS, No. 1, (18 de agosto de 2009); [Sentencia No. 0001-12-HD], en ROS, No. 949 (8 de mayo de 2013), [Sentencia No. 0001-13-HD], en ROSEC, No. 2 (5 de junio de 2017).

[462] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 00182-15-SEP-CC]; [Sentencia No. 0002-14-HD] en ROEC, No. 2 (5 de junio de 2017)

> jurisprudencialmente, pertenece a la esfera de la constitucionalidad. Esta primera distinción que a los ojos de los entendidos resulta hasta primigenia, es uno de los principales escollos con los que se enfrentan los profesionales del Derecho, pues aún en el Ecuador esta discriminación estrictamente conceptual se dificulta por el desconocimiento existente al respecto.[463]

El *habeas data* debe dirigirse a la protección de los derechos constitucionales de la personalidad de su titular, de tal forma que el no utilizarlo con esta finalidad significa una desnaturalización de la garantía, conforme señala en la cita que consta a continuación:

> [...] No se dirigió a ser un mecanismo de satisfacción urgente para que el legitimado activo pueda obtener conocimiento de sus datos personales; y, por otra, tampoco tuvo como principal finalidad la protección de sus derechos constitucionales de la personalidad, por lo cual, se produjo una desnaturalización de esta garantía jurisdiccional en tanto los documentos requeridos se pueden solicitar por medio de la diligencia de exhibición de documentos como acto preparatorio a la interposición de determinada acción judicial, por no estar sujetos al ámbito de protección que consagra el artículo 92 de la Constitución de la República.[464]

Para que opere el *habeas data* es necesario que la información solicitada sea de carácter personal; si es que se desea acceder a información de terceras personas, la acción procedente es la de exhibición de documentos conforme consta del análisis encontrado en la sentencia No. 0039-2007-HD, cuya parte pertinente consta a continuación:

> De lo indicado en el considerando anterior, se desprende también, que la acción de hábeas data tiene dos presupuestos que la hacen procedente, y que deben operar en forma relacionada, tales son: Que la información en poder del requerido debe pertenecer al solicitante, y que se considere de manera fundada, que la información puede llegar a afectar el honor, la buena reputación, la intimidad o irrogar daño moral a la persona. En este caso, la petición que hace el recurrente es sobre documentación referente a terceros, y se aprecia que la finalidad es la consecución de documentos para presentar acciones judiciales, por lo que desnaturaliza la acción de hábeas data. El actor debería presentar una acción de exhibición de documentos, lo cual se encuentra previsto en el Código de Procedimiento Civil.[465]

En sentencia No. 0046-2002-HD, que consta transcrita a continuación, se describe el contenido de las facultades que les corresponden a los titulares para el ejercicio del *habeas data* y con ello diferenciarlo de la acción de exhibición de documentos:

> […] es una garantía constitucional con objetivos muy precisos que permite el acceso a la información, se verifica la exactitud de la información del que la posee, se verifica el uso que el poseedor está dando a esa información, se impide que se difunda si ésta es errada, se cambia la información si es equivocada y se difunde la verdadera información entre aquellos a quienes el poseedor de ella la remitió o circuló, todo ello con el propósito de proteger o resguardar los derechos constitucionales subjetivos; (sic) Que, la exhibición de documentos normada en el Código de Procedimiento Civil procede para fundamentar una demanda o

[463] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0039-2008-HD], en ROS, No. 86 (5 de diciembre de 2008).

[464] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [sentencia No. 0001-11-HD], en ROSEC, No. 7, (2 de mayo de 2017).

[465] Ibíd., [Sentencia No. 0039-2007-HD], en ROS, No. 133 (10 de julio de 2009).

> contestarla, consecuentemente tiene un carácter probatorio para ser utilizado en un proceso civil como acto preparatorio o como diligencia sustanciada.[466]

En el mismo sentido, lo dispuesto por la Corte Constitucional, para el período de transición, en resolución No. 0070-2008-HD que señala que, el *habeas data* no es un procedimiento cautelar ordinario:

> "es un proceso ágil y expedito no es su objetivo ordenar se practiquen diligencias encaminadas a asegurar la existencia de documentos, no puede ser entendido como el mecanismo de orden cautelar por el que se anticipe a solicitar información o exhibición de documentos que pudieren servir de fundamento para presentar una demanda o para contestarla, porque para este fin existen mecanismos o actos preparatorios que han de ser materia de la acción correspondiente"[467].

Finalmente, se identifica la naturaleza del *habeas data* para que a través de la descripción de los derechos que protege se pueda distinguir a esta garantía constitucional de la exhibición de documentos que tiene fines probatorios, al tenor de la cita a continuación:

> […] la pretensión de los recurrentes no se relaciona con la verdadera función de la garantía constitucional del hábeas data, pues no se busca proteger la autodeterminación informativa de los recurrentes, al contrario, los recurrentes solicitan la exhibición de documentos de terceros, Es decir, no existe una vulneración a los derechos constitucionales objeto del hábeas data, como la autodeterminación informativa, la honra, el acceso a documentos sobre sí mismos, su familia o sus bienes, entre otros.[468]

6.1.1.8 Diferencia entre *habeas corpus y habeas data*

Si bien, no pareciera que pudiera existir ningún tipo de confusión entre estas dos garantías constitucionales, ya que el *habeas corpus* se refiere a la libertad física de las personas y en consecuencia muestra a la persona, mientras que el *habeas data* hace alusión a sus datos e información y pone a disposición estos, sin embargo, en la sentencia que a continuación se transcribe consta una clara diferenciación*:*

> Que, en el presente caso, el accionante menciona en su demanda que ha sido detenido sin ningún fundamento, y entre los documentos que solicita se encuentran las boletas constitucionales de encarcelamiento. Al respecto, nuestra Constitución es clara en distinguir al hábeas corpus y al hábeas data como dos tipos de acciones diferentes para la protección de los derechos garantizados por la misma: la primera se encuentra establecida en el artículo 93 de la Carta Magna, que señala: "Toda persona que crea estar ilegalmente privada de su libertad podrá acogerse al hábeas data..." Esta acción se interpone ante el Alcalde bajo cuya jurisdicción se encuentre el accionante, y está destinada a que se exhiba la orden de privación de libertad, no se establece que sean entregadas las boletas constitucionales de encarcelamiento al accionante, por obvias razones. El hábeas data, como queda dicho anteriormente, es una acción que se interpone para acceder a determinados documentos que

[466] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0046-2002-HD], en ROS, No. 66 (22 de abril de 2003).
[467] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [sentencia No. 0070-2008-HD], EN ROS, NO. 2 (20 DE AGOSTO DEL 2009); [SENTENCIA NO. 0001-13-HD], EN ROEC NO. 2 (05 DE JUNIO DE 2017)
[468] Ecuador, CORTE CONSTITUCIONAL, [Sentencia No. 1-17-HD], en ROEC No. 70 (29 de marzo de 2019)

> forman parte de bancos de datos, y que contienen información sobre el accionante o sobre sus bienes. Las dos tienen procedimientos distintos y finalidades distintas.[469]

6.1.1.9 Necesidad de afectación de derechos

Conforme señala la jurisprudencia que se cita a continuación para que proceda el *habeas data*, conforme la jurisprudencia de ese entonces, era necesario que se manifieste un daño o afectación a un derecho fundamental:

> La información a la que se puede acceder a través del Hábeas Data puede versar sobre la persona o sus bienes, pero debe ser estrictamente el tipo de información que afecte el derecho que garantiza esta acción constitucional como queda señalado.[470]

Como se analizó en líneas precedentes los derechos que se protegían mediante el *habeas data* "son el honor, la buena reputación, la intimidad o irrogar daño moral a la persona".[471]

6.1.1.10 Habeas data protege el derecho a la protección de datos personales

La sentencia que a continuación se transcribe fue dictada en el año 2002; es decir, antes de que en Ecuador se reconozca en la Carta Magna el derecho a la protección de datos personales. Sin embargo, dicha sentencia reconoce que el *habeas data* vela por este derecho fundamental. Lamentablemente, no existe univocidad al respecto y únicamente en otra sentencia, dictada seis años después, en el año 2008, se vuelve a mencionar este criterio jurisprudencial, por lo que entendemos no fue aceptado ni aplicado por los juzgadores de la época.

> El Hábeas Data permite a toda persona acceder a registros públicos o privados, en los cuales están incluidos sus datos personales o de su familia, para requerir su rectificación o la supresión de aquellos datos inexactos que de algún modo le pudiesen perjudicar en su honra, buena reputación e intimidad. El derecho a la protección de datos implica, a su vez, el derecho a conocer la existencia de ficheros o de información almacenada y el propósito o la finalidad que se persigue con ellos.[472]

---

[469] Ibíd., [Sentencia No. 021-HD-IS], en RO, No. 454 (15 de noviembre de 2001).
[470] Ibíd., [Sentencia No. 0033-2004-HD], en RO, No. 389 (30 de julio de 2004).
[471] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR,, [Sentencia No. 0039-2008-HD], en ROS, No. 86, de 5 de diciembre de 2008; Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0053-2004-HD], en RO, No. 389 (30 de julio de 2004); Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0019-2007-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0048-2007-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0003-2008-HD], en ROS, No. 133 (10 de julio de 2009); Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0005-2008-HD], en ROS, No. 68 (05 de agosto de 2008); Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0031-2008-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0038-2008-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0083-2008-HD], en ROS, No. 126 (9 de junio de 2009); [Sentencia No. 0001-2009-HD], en ROS, No. 111 (25 de marzo de 2009); [Sentencia No. 0004-09-HD], en ROS, No. 590 (14 de mayo de 2009).
[472] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0046-2002-HD], en ROS, No. 66 (22 de abril de 2003); Ecuador, CORTE CONSTITUCIONAL, [Sentencia No. 0051-08-HD], en ROS, No. 531 (18 de febrero de 2009). Ecuador, CORTE CONSTITUCIONAL, [Sentencia No. 1-17-HD], en ROEC No. 70 (29 de marzo de 2019)

Del texto, además se puede identificar un error conceptual pues solo procede el derecho de protección de datos personales sobre aquellos de los que se es titular, y por ende, no puede interponerse *habeas data* respecto de datos que sean propios de otros miembros de su núcleo familiar.

6.1.1.11 No procede *habeas data* cuando se pretende obstruir la justicia

No procede *habeas data* cuando los datos solicitados son de aquellos que la ley establece como necesarios, como por ejemplo aquellos indispensables para realizar la investigación procesal que permita la atribución de responsabilidad en un proceso penal; de tal manera que no deberá ser entregado si al hacerlo se vulnera o se puede obstruir la justicia.

> Que por el tipo de informes del que se trata, aunque en ellos se encontraren datos susceptibles de acceso de acuerdo a lo establecido por el artículo 94 de la Constitución, por las evidencias constantes en el expediente en folios 13 y 14, documento en el cual se señalan siete causas penales en las que se encuentra sindicado el accionante, entre ellas, muerte, asalto y robo, robo de vehículos y tenencia de armas, no procede que estos documentos sean entregados como lo pretende el peticionario, según lo establecido en la Ley de Control Constitucional, artículo 36: «No es aplicable el hábeas data [...] cuando pueda obstruir la acción de la justicia» [...] Por las características de la documentación solicitada y la condición del accionante de sindicado en varias causas penales, y además por cuanto él mismo señala en su demanda que «se evadió» una vez del centro en donde se encontraba detenido, esta Sala observa que efectivamente con la presente acción se pretende obstruir la acción de la justicia.[473]

6.1.2 Contenido, derechos y facultades del *habeas data*

6.1.2.1 Información personal

Para comprender qué se entiende por información personal se analizará la sentencia No. 0102-2004-HC[474] respecto de la pretensión de una persona de acceder a dos pagarés, firmados por la parte accionante y que se encuentran en poder de un Banco, y de conocer la finalidad o destino que esa institución bancaria ha dado a los mencionados documentos. Se considera que si los documentos fueron suscritos por la demandante, esta es información que concierne a su persona.

Asimismo, en sentencia No. 0007-2006-HD[475] se señala que la acción de *habeas data* garantiza el acceso a la información respecto de sus datos personales y patrimoniales que consta en instituciones. En consecuencia, si se desea acceder a hechos, circunstancias, procesos y actos ajenos a las personas y sus bienes, y que se refieren a la gestión municipal, se pueden acceder en ejercicio del derecho a la información, como consecuencia de la transparencia y publicidad que reclama la actividad pública, pero no del *habeas data*.

En suma, el *habeas data* procede únicamente de información personal por cuanto "la esencia del recurso de hábeas data es lograr la información veraz requerida por el accionante; situación distinta sería si es que terceros lo solicitan con la finalidad de causar daño, afectar el

[473] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR [Sentencia No. 021-HD-IS], en RO, No. 454 (15 de noviembre de 2001); [Sentencia No. 0015-2001-HD], en ROS, No. 380 (31 de julio de 2001); [Sentencia No. 0022-2004-HD], en RO, No. 353 (10 de junio de 2004); [Sentencia No. 0102-2004-HD], en RO, No. 531 (24 de febrero de 2005); [Sentencia No. 0011-2006-HD], en ROS, No. 335 (16 de agosto de 2006); Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0079-2008-HD], en ROS, No. 8 (4 de septiembre de 2009).
[474] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0102-2004-HC].
[475] Ibíd., [Sentencia No. 0007-2006-HD].

honor y en general para utilización maliciosa. En consecuencia, es obligación del juez respectivo garantizar el ejercicio del derecho a la información y hacer que se cumpla la particularidad del recurso. El juez está obligado a garantizar el ejercicio del derecho a la información personal de conformidad con lo que establecen los Arts. 39 y 40 de la Ley del Control Constitucional".[476] Toda vez que, conforme señala la sentencia No. 046-2002-HD, "es menester puntualizar que para que opere el hábeas data la información requerida debe pertenecer específicamente y con precisión a quien lo solicita toda vez que es una garantía constitucional con objetivos muy precisos",[477] refiriéndose a que solo su titular puede saber si el dato es correcto o errado, y por ende amerita rectificación, o si este puede haberse difundido o difundirse y causarle un perjuicio.

En un caso que conmocionó a la ciudad de Quito, una pareja al presentar a su hijo en la embajada para solicitar la nacionalidad de dicho país, resultó no ser hijo biológico de sus progenitores. Entonces, se solicitó que se exhibiera toda la documentación referente a los nacimientos de todos los infantes nacidos en determinada fecha y hospital, así como los nombres de las madres de dichos infantes, su historia clínica y el tratamiento que recibieron, con el objeto de conocer su identidad. En sentencia de mayoría se decidió negar la acción de *habeas data* presentada "por cuanto los datos referidos debían pertenecer específicamente y con precisión a quien lo solicita toda vez que es una garantía constitucional con objetivos muy precisos".[478]

6.1.2.2 El fin que la persona le dé a la información no es trascendente para el acceso

La sentencia No. 0102-2004-HC[479] establece que el fin que la persona dé a la información es intrascendente para atender el requerimiento de acceso a la información mediante la garantía del *habeas* data. Por tanto, la excepción planteada, respecto a la improcedencia de la acción por considerar que bien pudo solicitarse una exhibición de documentos, se desestima.

6.1.2.3 No se puede solicitar acceso a información que se conoce

Al respecto, el alcance del derecho al acceso a la información personal mediante el *habeas data* fue analizado en la sentencia No. 0070-2003-HD,[480] la cual señala que "no se puede solicitar información que se conoce". La sentencia indica que los accionantes obtuvieron un crédito para compra de vehículo y debido a la dolarización restructuraron la deuda. Los actores proponen acción de *habeas data* para que se otorgue información sobre el destino de los títulos de la deuda no devueltos. El Tribunal Constitucional considera que en este caso los deudores saben y, así lo demuestran en el contenido de su recurso, cuánto deben a la institución financiera y cómo fue reestructurada la deuda, por lo que no pueden solicitar por medio del *habeas data* información que ya conocen.

---

[476] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0013-08-HD], en ROS, No. 127 (15 de junio de 2009); Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0015-2001-HD], en ROS, No. 380 (31 de julio de 2001; [Sentencia No. 0018-2001-LID], en ROS, No. 370 (17 de julio de 2001). Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0048-2007-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0001-08-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0084-08-HD], en ROS, No. 112 (27 de marzo de 2009); [Sentencia No. 0001-2009-HD], en ROS, No. 111 (25 de marzo de 2009).
[477] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 046-2002-HD], en ROS, No. 66 (22 de abril de 2003).
[478] Ibíd., [Sentencia No. 0033-2004-HD].
[479] Ibíd., [Sentencia No. 0102-2004-HC].
[480] Ibíd., [Sentencia No. 0070-2003-HD], en RO, No. 271 (11 de febrero de 2004).

6.1.2.4 No se puede solicitar *habeas data* sobre información inexistente

La sentencia 0023-08-HD señala expresamente que "los accionantes no pueden pretender la entrega de documentación o información inexistente, o que por no contener datos o información personal deberían ser requeridas por otras vías".[481] Si bien esta sentencia resulta obvia respecto de que no se puede entregar información que no consta en una base de datos; sin embargo, no puede ser motivo de rechazo inicial porque la persona tiene derecho a solicitar el acceso a su información personal, ya que nunca tendrá la certeza de su existencia. Además, esta negativa del titular del fichero o base de datos emplazados debiera ser verificada por entes técnicos que garanticen el ejercicio del derecho; de ahí la necesidad de constituir organizaciones especializadas como ocurre en otros países.

6.1.2.5 Necesidad de especificar a qué información se desea acceder

El criterio descrito en estas sentencias, respecto de la necesidad de especificar el tipo de información que desea accederse mediante el *habeas data* es cuestionable, ya que no se puede pedir al legitimado activo un nivel de precisión de la información que por obvias razones desconoce, precisamente por no tener acceso, por no estar en sus manos o desconocer la forma en la que se trata o almacena los datos o la información ya sea en soporte físico o virtual, por parte de una persona natural o jurídica; de ahí que por ello solicita el *habeas data*.

Aunque criticable, es menester citar la mencionada sentencia para su análisis:

> En su escrito inicial el accionante no determina ni especifica el tipo de documento requerido, la fecha de expedición del mismo, ni la persona sea ésta natural o jurídica que la confirió. Con ello no justifica de manera alguna, que la documentación que solicita se refiera a su persona o a sus bienes. [...] De conformidad con el texto del escrito ingresado a esta Sala el día jueves 3 de junio del 2004 a las 15h25, el propio actor argumenta y expresa: "4.-...si solicito información es porque no recuerdo en forma detallada de que información sobre mí mismo o mis bienes tiene la entidad requerida". En el numeral 5 del mismo escrito, dice: "Por lo que la Asociación Agrícola Los Arenales desde el momento mismo en que fui socio entre otros documentos que sobre mí mismo debe poseer es lógico que debe tener la documentación sobre mi ingreso, aportaciones, documentos que yo no recuerdo, documentos por los cuales he dejado de ser socio, ya que no los recuerdo, etc. [...] La información a la que se puede acceder a través del Hábeas Data, debe ser estrictamente el tipo de información que afecte el derecho que garantiza esta acción constitucional como queda señalado por lo que, al no ser especificada, mal se puede hacer garantizar su cumplimiento.[482]

De la simple lectura de esta jurisprudencia se colige que existe un desconocimiento del derecho de acceso que es parte del *habeas data*, pues este solo se garantiza en la medida en la que los responsables de los ficheros, sujetos pasivos de la acción, entreguen no solo aquella información específica que le fuera solicitada, sino toda la información que está en su poder. Solo de esta forma se puede verificar que los datos y la información en manos de otras personas no afectan sus derechos fundamentales.

---

[481] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0023-08-HD], en ROS, No. 535 (26 de febrero de 2009).

[482] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0033-2004-HD], en RO, No. 389 (30 de julio de 2004; [Sentencia No. 0053-2004-HD], en RO, No. 389, de 30 de julio de 2004).

6.1.2.6 Derechos y facultades del *habeas data*

Tal como sucede con los derechos ARCO, en el derecho a la protección de datos personales la norma tiene por finalidad proteger otros derechos constitucionales que pueden verse afectados por datos inexactos o equivocados. De tal forma que para la sentencia 046-2002-HD se describe las facultades del *habeas data*, puesto que este "permite el acceso a la información, se verifica la exactitud de la información del que la posee, se verifica el uso que el poseedor está dando a esa información, se impide que se difunda si ésta es errada, se cambia la información si es equivocada y se difunde la verdadera información entre aquellos a quienes el poseedor de ella la remitió o circuló, todo ello con el propósito de proteger o resguardar los derechos constitucionales subjetivos".[483]

En alusión a la normativa de la época la sentencia recoge los derechos-facultades del *habeas data* pues señala que se refieren al acceso, rectificación, eliminación, no divulgación o verificación. El texto de la sentencia 0042-2005-HD dice expresamente:

> [...] de acuerdo con el artículo 35 de la Ley de Control Constitucional, tiene por objeto: a) obtener del poseedor de la información que éste le proporcione al recurrente, en forma completa, clara y verídica; b) obtener el acceso directo a la información; c) obtener de la persona que posee la información que la rectifique, elimine o no la divulgue a terceros; y, d) obtener certificaciones o verificaciones, sobre que la persona poseedora de la información la ha rectificado, eliminado, o no lo ha divulgado.[484]

Por eso es que el contenido de la garantía constitucional a la época es el de reserva, acceso, rectificación, supresión o actualización conforme reza del siguiente texto:

> La Constitución y la doctrina establece dos pilares fundamentales sobre los que se asienta el *habeas data*, el primero el derecho a la reserva de los datos que las personas tienen sobre si mismas o sus bienes en instituciones públicas o privadas, así como el acceso a los mismos y su supresión, rectificación o actualización. El tratadista Enrique Falcón sobre esta acción dice: «Es un remedio urgente para que las personas puedan obtener: el conocimiento de los datos a ellos referidos y de su finalidad, que conste en el registro o bancos de datos públicos o privados y en su caso para exigir la supresión, rectificación, confidencialidad o actualización de aquellos».[485]

6.1.2.7 Derecho de acceso

[483] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 046-2002-HD], en ROS, No. 66 (22 de abril de 2003); [Sentencia No. 021-HD-IS], en RO, No. 454 (15 de noviembre de 2001); [Sentencia No. 0046-2002-HD], en ROS, No. 66 (22 de abril de 2003).

[484] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0042-2005-HD], en ROS, No. 309 (10 de julio de 2006); Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0019-2007-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0032-07-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia 0044-2007-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0065-2008-HD], en ROS, No. 100 (11 de febrero de 2009); [Sentencia No. 0067-2008-HD], en ROS, No. 126 (9 de junio de 2009); [Sentencia No. 0005-09-HD], en ROS, No. 129 (19 de junio de 2009); [Sentencia No. 0011.2009-HD], en ROS, No. 13 (08 de octubre de 2009).

[485] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0044-2008-HD], en ROS, No. 87 (11 de diciembre de 2008); [Sentencia No. 0007-2009-HD], en ROS, No. 10 (11 de septiembre de 2009); [Sentencia No. 0030-2008-HD], en ROS, No. 124 (27 de mayo de 2009); [Sentencia No. 0080-2008-HD], en ROS, No. 129 (27 de mayo de 2009).

El *habeas data* como garantía constitucional permite el ejercicio de diversos derechos, para lo cual es necesario efectivizar el derecho de acceso por cuanto solo a través de este, el titular del dato puede conocer la información que un responsable de tratamiento tiene de él, su uso y su propósito y con este conocimiento arbitrar el ejercicio de otros derechos. Para esto la jurisprudencia, como consta a continuación, determina que el poseedor de la información deberá entregar la información del titular en los términos establecidos en la norma constitucional.

> Que, el hábeas data es una garantía constitucional que tiene por objeto proteger el acceso a la información personal, así como el derecho a la honra, a la buena reputación y a la intimidad personal y familiar, y en consecuencia es un derecho de toda persona acceder a los documentos, banco de datos o informes que sobre sí misma, o sus bienes consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellas y su propósito; de ello, se advierte que toda persona natural o jurídica está facultada para requerir del poseedor de la información, que haga relación a ella y que le sea entregada en los términos que establece la norma constitucional.[486]

A través del *habeas data* concebido como garantía pero también como derecho se fortalece la democracia por que incentiva la transparencia del tratamiento, garantizando con ello al titular de la información el seguimiento de las finalidades para las que sus datos fueron recolectados, y a la par, permitir el ejercicio de otra serie de derechos fundamentales que conjugan la garantía.

> Precisamente en el campo constitucional de disponer de ciertos mecanismos jurídicos que, de modo directo e inmediato sirven para tutelar o garantizar los derechos de las personas, tales como el derecho a dirigir peticiones y a recibir atención y las respuestas pertinentes; el derecho a acceder a fuentes de información objetiva y verás, plural y oportuna sobre sí misma y en términos generales siempre que no afecte al sigilo profesional, no obstruya la acción de la justicia. [487]

Del texto transcrito se desprende que es parte de este derecho – garantía que el acceso se realice a fuentes objetivas, veraces, plurales y oportunas. Es decir, se evidencia el principio de calidad de datos como elemento esencial que faculte a los titulares de los datos su protección integral.

6.1.2.8 Derecho de rectificación

Uno de los derechos que consta descritos en la garantía constitucional del *habeas data* es el de rectificación, como consta en la sentencia No. 0066-08-HD, mediante la cual un estudiante solicita a una universidad el acceso, la revisión y rectificación de sus calificaciones:

> El hábeas data permite a toda persona acceder a registro públicos o privados, en los cuales están incluidos sus datos personales, como lo son las calificaciones de las pruebas presenciales y a distancia solicitadas por el accionante, para requerir su rectificación, la supresión de aquellos datos inexactos que de algún modo le pudieran perjudicar en su honra, buena reputación e intimidad; derecho que no se puede permitir sean conculcados a pretexto de proteger la autonomía universitaria, que de ninguna manera se habría visto afectada, si la Universidad [...], habría cumplido con su obligación de presentar la información solicitada y permitido con ello determinar si realmente la información que aparece en la página *web site*,

[486] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0079-2008-HD], en ROS, No. 8 (4 de septiembre de 2009); [Sentencia No. 0059-2008-HD], en ROS, No. 137 (4 de agosto de 2009).
[487] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0066-08-HD], en ROS, No. 135 (17 de julio de 2009.

> es verás (sic por veraz) o errada como afirma el accionante, al ejercer su legítimo derecho a rectificar, que es la posibilidad del titular afectado de que los datos sobre su persona al ser incorrectos, inexactos u obsoletos sean rectificados en la medida de que al ser ajenos a la realidad, le puedan causar perjuicios. [488]

Como se ve es indispensable el acceso a los datos personales para ejercer los derechos de actualización y rectificación, para que los legitimados activos conozcan con certeza de la información que consta en el fichero con la finalidad de contrastarla con aquella que consideran actual o cierta, y en consecuencia proceda o no su reclamo.

En el mismo sentido, la sentencia No. 46-2002 señala que el derecho de rectificación opera cuando los datos son incorrectos, inexactos y obsoletos:

> El derecho a acceder, que permite a los afectados averiguar el contenido de la información registrada, o participar de la información que sobre la imagen o concepto de ellos se tenga; y el derecho a rectificar, que es la posibilidad del titular afectado, de que los datos sobre su persona o de su entorno familiar al ser incorrectos, inexactos u obsoletos, sean rectificados en la medida en que, al ser ajenos a la realidad, le pueden causar perjuicio a su familia o a sus bienes.[489]

6.1.2.9 Se rectifican datos personales; no se pueden rectificar obligaciones o derechos pendientes de reconocimiento judicial

En la cita que consta a continuación se visibiliza una confusión respecto de la procedencia del *habeas data*, puesto que esta garantía constitucional permite rectificar únicamente datos o información personal. No puede ser utilizada para enervar la justicia e intentar favorecerse de una rectificación respecto de obligaciones o derechos que aún están pendientes de reconocimiento judicial.

> [...] si no existe un derecho definido, a favor de los recurrentes, pues precisamente está en discusión la existencia o no de la obligación, y no solo se ha solicitado el «tener acceso» a la información, con lo cual los actores ya podrían hacer valer sus derechos ante las autoridades competentes, para que sean ellas, las autorizadas por la ley, y en el caso de que se trate de conflictos sometidos a la jurisdicción de un Juez, sea éste, quien o quienes determinen la existencia o no de obligaciones, sino que se ha solicitado que en aplicación del literal c) del Artículo 35 de la ley referida, se rectifiquen los asientos contables. Sobre esto último, el que por medio de un Hábeas Data, se logre que en definitiva, «a criterio de los actores», se modifiquen asientos contables de una obligación, se establezca la cancelación de una obligación con Convenios de dación en pago, es un fin ajeno a la naturaleza de la acción de Hábeas Data. Más bien, por el contrario, en realidad puede provocar que se enerve la acción de la justicia.[490]

[488] Ibíd., [Sentencia No. 0066-08-HD], en ROS, No. 135 (17 de julio de 2009); [Sentencia No. 0068-08-HD], en ROS, No. 535 (26 de febrero de 2009); [Sentencia No. 0074-2008], en ROS, No. 8 (4 de septiembre de 2009); [Sentencia No. 0076-2008-HD], en ROS, No. 111 (25 de marzo de 2009).
[489] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0046-2002-HD], en ROS, No. 66 (22 de abril de 2003); Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0051-08-HD], en ROS, No. 137 (26 de noviembre de 2008). [Sentencia No. 0038-2008-HD], en ROS, No. 133 (10 de julio de 2009).
[490] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0015-2006-HD], en ROS, No. 11 (30 de enero de 2007).

6.1.3 Aspectos procesales del *habeas data*

6.1.3.1 El legitimado activo puede ser individual o plural

Respecto, de si el recurso de *habeas data* debía ser presentado de manera individual porque se pretende tener acceso a información personal, en sentencia No. 0070-2003-HD se señala que sí se puede presentar en conjunto por personas naturales, pues:

> [...] el hecho de que la norma de la Constitución esté redactada en singular, no significa que la demanda no pueda ser presentada por varias personas, así como el hecho de estar la norma de la Ley del Control Constitucional redactada en plural, no significa que solamente varias personas puedan proponer la acción. No existe ni en la Constitución ni en la Ley del Control Constitucional, impedimento alguno para que varias personas, nombrando procurador común, demanden contra una misma autoridad o persona jurídica o natural de derecho privado, como en la especie, cuando los datos sobre todas ellas se encuentren en los archivos del o la demandada, por lo tanto, es factible la proposición de la acción de hábeas data por varias personas. [491].

6.1.3.2 No se necesita accionar contra el que consta como representante legal de la institución

La sentencia No. 0102-2004-HC[492] señala que la parte accionante del *habeas data* no está obligada a conocer y presentar la acción contra quien es el representante legal de la institución, pues se garantiza celeridad e inmediatez en el acceso al derecho. Basta con que esa persona pertenezca a la institución.

6.1.3.3 El legitimado pasivo puede ser persona natural o jurídica pública o privada

Por su parte, en sentencia No. 0102-2004-HC[493] se aclara que el *habeas data* puede ser interpuesto contra instituciones públicas, personas naturales o personas jurídicas privadas. El caso analizado tenía como sujeto pasivo a una persona jurídica privada (Banco) que mantenía en su poder documentos relacionados con la parte accionante. En el mismo sentido, otras

---

[491] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0070-2003-HD], en RO, No. 271 (11 de febrero de 2004); [Sentencia No. 0015-2001-HD], en ROS, No. 380 (31 de julio de 2001); [Sentencia No. 0018-2001-LID], en ROS, No. 370 (17 de julio de 2001); Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0028-2007-HD], en ROS, No. 133 (10 de julio de 2009); [Sentencia No. 0032-07-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0001-2008-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0005-2008-HD], en ROS, No. 68, de 05 de agosto de 2008; [Sentencia No. 0010-2008-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0020-2008-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0034-08-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0041-08-HD], en ROS, No. 590 (14 de mayo de 2009); [Sentencia No. 0045-08-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0049-2008-HD], en ROS, No. 137 (26 de noviembre de 2008); [Sentencia No. 0060-08-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0061-2008-HD], en ROS, No. 120 (28 de abril de 2009); [Sentencia No. 0070-2008-HD], en ROS, No. 2 (20 de agosto de 2009); [Sentencia No. 0077-2008-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0081-2008-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0084-08-HD], en ROS, No. 112 (27 de marzo de 2009); [Sentencia No. 0011-2009-HD], en ROS, No. 13 (8 de octubre de 2009); [Sentencia No. 0012-2009-HD], en ROS, No. 13 (8 de octubre de 2009); [Sentencia No. 0013-2009-HD], en ROS, No. 13 (8 de octubre de 2009).

[492] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0102-2004-HD], en RO, No. 531 (24 de febrero de 2005).

[493] Ibíd., [Sentencia No. 0102-2004-HD], en RO, No. 531 (24 de febrero de 2005).

resoluciones señalan que las personas naturales o personas jurídicas públicas o privadas pueden ser legitimados pasivos del *habeas data*.[494]

6.1.3.4 Imposibilidad de presentar incidentes

En la sentencia No. 0102-2004-HC[495] se señala que el *habeas data*, por constituirse una garantía del derecho a la información, deberá atenerse a los principios de celeridad e inmediatez, sin que pueda admitirse incidentes de ninguna clase en estos procesos.

6.1.3.5 Los terceros son legitimados activos en el *habeas data* aunque no pretendan causar daño

Por cuanto la información protegida por el *habeas data* es aquella de carácter personal "mediante esta acción no puede ser solicitada información sobre terceras personas sino solo sobre los accionantes, aunque con ello no se persigan causar daño, afectar el honor y en general utilizar dicha información con fines maliciosos".[496] La finalidad de quien solicita el *habeas data* si bien es importante, no habilita por sí sola, pues solo procede respecto de los datos de los que se es titular.

6.1.3.6 Necesidad de especificar el tipo de documento requerido

La sentencia No. 0033-04-HD[497] señala que es obligación del accionante de *habeas data* determinar o especificar el tipo de documento requerido, la fecha de expedición del mismo, la persona sea esta natural o jurídica que la confirió. Con ello no justifica, de manera alguna, que la documentación que solicita se refiera a su persona o a sus bienes. La información a la que se puede acceder *mediante el habeas data* puede versar sobre la persona o sus bienes, pero debe ser estrictamente el tipo de información que afecte el derecho que garantiza esta acción constitucional como queda señalado.

Al respecto, resulta absurdo, bajo el criterio de efectiva vigencia del *habeas data*, solicitar que el peticionario describa todos los datos del documento para que la acción de datos prospere. Más aun, porque es inválida para justificar que el demandando desconocía las precisiones de los documentos; al respecto véase la constancia en la sentencia de aquella cita

---

[494] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0102-2004-HD], en RO, No. 531 (24 de febrero de 2005); Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0020-2008-HD], en ROS, No. 137 (4 de agosto de 2009). [Sentencia No. 0041-08-HD], en ROS, No. 590 (14 de mayo de 2009); [Sentencia No. 0068-08-HD], en ROS, No. 535 (26 de febrero de 2009); [Sentencia No. 0011-2009-HD], en ROS, No. 13 (8 de octubre de 2009); [Sentencia No. 0012-2009-HD], en ROS, No. 13 (8 de octubre de 2009); [Sentencia No. 0013-2009-HD], en ROS, No. 13 (8 de octubre de 2009).

[495] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0102-2004-HD], en RO, No. 531 (24 de febrero de 2005); [Sentencia No. 0020-2008-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0041-08-HD], en ROS, No. 590 (14 de mayo de 2009); [Sentencia No. 0068-08-HD], en ROS, No. 535 (26 de febrero de 2009); [Sentencia No. 0011-2009-HD], en ROS, No. 13 (8 de octubre de 2009); [Sentencia No. 0012-2009-HD], en ROS, No. 13 (8 de octubre de 2009); [Sentencia No. 0013-2009-HD], en ROS, No. 13 (8 de octubre de 2009).

[496] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0023-08-HD], en ROS, No. 535 (26 de febrero de 2009); [Sentencia No. 0018-2007-HD], en ROS, No. 137 (4 de agosto de 2009); [Sentencia No. 0011-09-HD], en ROS, No. 13 (8 de octubre de 2009); [Sentencia No. 0012-2009-HD], en ROS, No. 13 (8 de octubre de 2009); [Sentencia No. 0013-2009-HD], en ROS, No. 13 (8 de octubre de 2009).

[497] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0033-2004-HD].

extraída de una escrito ingresado a la Sala en el que el propio actor expresa: "4.-…si solicito información es porque no recuerdo en forma detallada de qué información sobre mí mismo o mis bienes tiene la entidad requerida...". En el numeral 5 del mismo escrito dice: "Por lo que la Asociación Agrícola Los Arenales desde el momento mismo en que fui socio entre otros documentos que sobre mí mismo debe poseer es lógico que debe tener la documentación sobre mi ingreso, aportaciones, documentos que yo no recuerdo, documentos por los cuales he dejado de ser socio, ya que no los recuerdo…".[498]

Al contrario, justamente de esta aseveración de la parte se materializa la necesidad de que esta acción no obligue al peticionario a conocer y precisar de antemano la información. Sino que sea la entidad, que tiene a su disponibilidad, debidamente organizada e incluso automatizada la información de las personas, porque es imposible y se gravaría en exceso a un particular el exigirle memoria y recuento absoluto de todas las actividades y documentos que las detallan. Pero, en cambio, es obligatorio no solo por criterio organizacional, sino hasta por cumplimiento de la normativa societaria que las instituciones mantengan archivos organizados.

6.1.3.7 No cabe incidentes en el proceso de *habeas data*

Por el tipo de daño en diversos derechos fundamentales que produce la falta de actualización, equivocación, difusión no autorizada de datos personales, entre otras transgresiones en el tratamiento de datos personales, los procesos previstos en la normativa para impedir su propagación o perpetuar el daño deben ser expeditos. En tal sentido, "El hábeas data constituye garantía del derecho a la información, reconocido por la Carta Política, la Ley de Control Constitucional, en el artículo 59 determina que deberá atenerse a los principios de celeridad e inmediatez, sin que pueda admitirse incidentes de ninguna clase en estos procesos".[499]

6.2 Jurisprudencia sobre protección de datos personales y *habeas data* desde la Constitución de 2008

A partir de la Constitución de 2008, la Corte Constitucional tiene la facultad de dictar resoluciones de aplicación generalmente obligatoria, ya que es necesario "el ejercicio de un control constitucional amplio y pleno, para dar efectiva vigencia a los derechos constitucionales y humanos y a la supremacía constitucional"[500].

En tal virtud, se conciben varias de las competencias dispuestas en el artículo 436 de la CRE y que constan a continuación:

a) numeral 1, referente a la interpretación con carácter vinculante de la Constitución y de los tratados internacionales de derechos humanos ratificados por el Estado ecuatoriano[501];

---

[498] Ibíd.

[499] Ecuador, TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0102-2004-HD], en RO, No. 531 (24 de febrero de 2005).

[500] CORTE CONSTITUCIONAL, [Sentencia No. 00182-15-SEP-CC].

[501] Ibíd. "La Corte Constitucional desde la vigencia de la Constitución del 2008, asume el rol garante de la Constitución dirigido principalmente hacia la protección de los derechos, superando la mera aplicación de la legalidad por el análisis de constitucionalidad del asunto controvertido, en ejercicio de las competencias que la Carta Suprema le asigna a este organismo. En tal virtud, el Art. 436 numeral 1 preceptúa: La Corte Constitucional ejercerá, además de las que le confiere la ley, las siguientes atribuciones: 1. Ser la máxima

b) numeral 3, relativo a la declaración de oficio de la inconstitucionalidad de normas conexas, cuando en los casos sometidos a su conocimiento concluya que una o varias de ellas son contrarias a la Constitución; y, [502]
c) numeral 6, sobre la generación de precedentes jurisprudenciales obligatorios.

En cumplimiento de las citadas atribuciones, analizaremos la jurisprudencia vinculante que ha generado la Corte Constitucional respecto del derecho a la protección de datos personales y del *habeas data*.

6.2.1 Precedente jurisprudencial obligatorio:

Conforme se señaló anteriormente, desde la Constitución de Montecristi de 2008, la jurisprudencia pasa a ser fuente formal del derecho. De ese modo, aquella que luego de un proceso de selección se integra al sistema de precedentes jurisprudenciales tiene efectos obligatorios de aplicación general.

Debido al numeral 6 del artículo 436 de la CRE la Corte Constitucional tiene competencia expresa para expedir sentencias que constituyan jurisprudencia obligatoria, para lo cual dictará reglas o *ratio decidendi*, cuyo contenido se vuelve vinculante para jueces de inferior o de igual jerarquía.

El procesamiento de cada una de las sentencias que integran el sistema de precedentes de la jurisprudencia constitucional es posible mediante la identificación en el texto de: a) la *ratio decidendi*, que es la que tendrá fuerza vinculante de carácter general y consiste en los motivos principales o razones para la toma de decisión por parte del tribunal; b) la *decisum*, que consta en la parte resolutiva; y c) los *obiter dicta*, que son argumentos o análisis que no tienen efecto vinculante pero que instruyen la decisión del tribunal.[503]

En el período comprendido desde 2008 hasta 2019, fecha de corte de esta investigación, existen dos sentencias de carácter vinculante dictada por la Corte Constitucional. La primera de ella, la sentencia es la No. 001-14-PJO-CC, dictada por la Corte Constitucional del Ecuador que se analizará a continuación, mientras que la otra que también genera efectos obligatorios, en virtud de otras de las atribuciones propias de la máxima Corte, la sentencia No. 00182-15-SEP-CC, se examinará posteriormente.

Esta sentencia resuelve varias inquietudes respecto de una problemática específica acerca de la titularidad de las personas jurídicas de los derechos fundamentales. Además, los

---

instancia de interpretación de la Constitución, de los tratados ratificados por el Estado ecuatoriano, a través de sus dictámenes y sentencias. Sus decisiones tendrán carácter vinculante. De esta forma se puede evidenciar la vocación de la Corte Constitucional como órgano de cierre de la justicia constitucional y por este motivo le corresponde, como manifiesta la Carta Suprema, ser el máximo organismo de control, interpretación constitucional y administración de justicia en esta materia".

[502] Ibíd. "Una de las atribuciones fundamentales de la Corte Constitucional es la del control abstracto de constitucionalidad, que se manifiesta en la potestad de este Organismo para declarar la inconstitucionalidad de las normas infraconstitucionales, por la necesidad de precautelar la supremacía constitucional y evitar posibles vulneraciones a derechos que puedan producirse como consecuencia de la aplicación de las normas contrarias a la Constitución. La competencia contenida en el numeral 3 del artículo 436 de la Constitución de la República se refiere a la declaratoria de inconstitucionalidad de las normas conexas, potestad que requiere de un comportamiento más activo por parte de la Corte Constitucional para efectuar de manera oficiosa el control de disposiciones normativas que comporten una vulneración a los derechos constitucionales y a los demás contenidos de la Norma Fundamental".

[503] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, *Protocolo para la Elaboración de Precedentes Constitucionales Obligatorios*, Resolución No. 4 - RA 2010 (5 de agosto de 2010).

argumentos desarrollados a lo largo de la decisión dejan claro que pretenden organizar, sistematizar y eliminar, al menos referencialmente, ciertas contradicciones suscitadas en los doce años en los que no existió jurisprudencia uniforme sobre el *habeas data*.

Asimismo, llama la atención que, pudiendo resolver otros elementos relativos al contenido esencial del derecho a la protección de datos personales, la sentencia se limite a resolver cuestiones limitadas a la garantía constitucional *habeas data*, en especial a su parte procedimental. Aunque, en la parte denominada *obiter dicta*, la sentencia menciona varios aspectos relativos al derecho fundamental, que no son de obligatorio cumplimiento sino meramente orientativos para jueces y tribunales.

6.2.1.1 *Obiter dicta:* efecto meramente referencial

A continuación, constan el análisis de la resolución obligatoria, No. 001-14-PJO-CC, en el cual se han clasificado los *obiter dicta* por temática y subtema para su respectivo análisis:

6.2.1.1.1 Sobre titulares y legitimados activos del derecho a la protección de datos personales y *habeas data*

1	**Generalización del término persona**	“En el caso del Ecuador, dicho parámetro se cumple con pertenecer a alguno de los géneros «personas», «comunidades», «pueblos», «nacionalidades», « colectivos». Como se puede advertir de una interpretación literal del texto constitucional, entonces, el término «personas», en tanto se refiere a la titularidad de los derechos constitucionales, no debe excluir a priori a una especie del género, como son las personas jurídicas”.
2	**Las personas jurídicas no pueden ser titulares de derechos cuyo ejercicio necesitan de un titular corpóreo con características bilógicas o psicológicas**	“Se podrá, sin duda, oponer a la conclusión anterior el que existen derechos constitucionales cuyo ejercicio no puede darse por parte de una persona jurídica, debido a sus características propias, distintas a las de un ente corpóreo, con características biológicas y psicológicas propias de los seres humanos. Un ejemplo, de entre muchos que se podrían presentar en apoyo a tal afirmación, es el derecho a la integridad psíquica reconocido en el artículo 66 numeral 3 literal a de la Constitución de la República. Empero, es criterio de esta Corte que el hecho de que ciertos derechos constitucionales no puedan ser ejercidos por alguno de los sujetos, no constituye una exclusión respecto de su calidad de tales. Dicho criterio ha sido expuesto por esta Corte en varias ocasiones en los casos de garantías que ha conocido. Por ejemplo, en la sentencia No. 068-10-SEP-CC, la Corte Constitucional...”
3	**Personas jurídicas pueden ser legitimados activos de las acciones constitucionales**	“en relación al aspecto adjetivo de la legitimación activa para invocar la acción de *habeas data*. Tal aspecto es importante, pues el concepto de derecho constitucional lleva indisolublemente aparejadas las nociones de exigibilidad y de justiciabilidad. Así, no tendría uso práctico alguno llegar a la conclusión que las personas jurídicas o por extensión, cualquiera de los sujetos mencionados en la Constitución de la República, son titulares de determinado derecho constitucional si ellas no tuvieren la posibilidad de reivindicarlo ante los órganos públicos responsables de su tutela. Por otro lado, esta Corte considera que las reflexiones que a continuación se detallan, comportan la distinción necesaria entre los conceptos de titularidad y legitimación activa, muchas veces confundidos en la praxis judicial”.

4	**La legitimación activa del *habeas data* se reduce solo al titular del derecho por sus propios derechos o como representante legitimado para el efecto**	"En lo concerniente a la legitimación activa para la presentación de las garantías jurisdiccionales de los derechos constitucionales, la regla general es que esta tenga el carácter de abierta, a modo de permitir el mayor campo posible de exigibilidad y un cierto nivel de conciencia social y solidaria ante las vulneraciones a derechos constitucionales. Sin embargo, en el caso del hábeas data, existen derechos en conflicto que pueden verse seriamente lesionados con una disposición que reconozca la legitimación activa abierta. Si no existe un acto de voluntad expreso que permita al legitimado activo comparecer a nombre del titular de los derechos constitucionales, el derecho a la intimidad y otros que dependen de la confidencialidad de la información personal estarían desprotegidos contra el uso malicioso de la acción. Es por ello que el mismo artículo 92 reduce la legitimación activa a " [t]oda persona, por sus propios derechos o como representante legitimado para el efecto...".
5	**Diferencias entre acceso a la información pública y *habeas data***	"el objeto del derecho a acceder a la información pública es diferente al protegido por la acción de hábeas data, encaminada a la protección de los datos personales, por lo que la misma Constitución de la República previó la existencia de una garantía jurisdiccional particular, denominada precisamente «acción de acceso a la información pública». Tal es así, que los datos personales, en gran parte de los casos, están protegidos por la excepción de confidencialidad al principio de publicidad de la información".

6.2.1.1.2 Sobre la naturaleza jurídica del derecho a la protección de datos personales

1	**El *habeas data* protege varios derechos**	"Una vez despejadas las dudas respecto de objetos extraños al ámbito de protección del hábeas data en el presente caso, es hora de analizar qué derecho protege de manera propia sin descartar que, dependiendo del caso, se hallen involucrados derechos conexos que también sean protegidos, en razón del principio de interdependencia. Para ello, es necesario hacer referencia a lo dispuesto en el artículo 66 numeral 19 de la Carta Suprema".
2	**Derecho a la protección de datos personales protege principios, derechos y garantías relacionados con la información personal**	"El derecho a la protección de datos personales tiene un contenido complejo y comporta diversas dimensiones relacionadas con la información «personal». Dicho criterio está expresado en la doctrina por el criterio de Oscar Puccinelli, quien señala lo siguiente: [P]or derecho a la protección de datos se propone entender la suma de principios, derechos y garantías establecidos en favor de las personas que pudieran verse perjudicadas por el tratamiento de los datos nominativos a ella referidos".

3	**La autodeterminación informativa es objeto de protección del *habeas data***	"Como bien refiere el autor, el derecho a la protección de datos -y específicamente, su elemento denominado «autodeterminación informativa-», tiene un carácter instrumental, supeditado a la protección de otros derechos constitucionales que se pueden ver afectados cuando se utilizan datos personales, como puede ser la intimidad, la honra, la integridad psicológica, etc. La autodeterminación informativa como objeto de protección del hábeas data y su carácter instrumental han sido reconocidos por esta Corte en el contexto de la norma constitucional de 1998, en varias sentencias. El contenido de este componente del derecho a la protección de datos personales es, según la Corte Constitucional, para el período de transición, «mantener el control de los datos que existan sobre una persona o sobre sus bienes, y para proteger el derecho a la honra, a la buena reputación y a la intimidad personal y familiar»".
4	**El *habeas data* tiene carácter instrumental porque mediante la autodeterminación informativa se protegen otros derechos**	
5	**Elementos que conforman la autodeterminación informativa**	"La autodeterminación informativa está supeditada, entonces, a la existencia de información que atañe a determinado sujeto y a la necesidad de que este tenga una esfera mínima de actuación libre respecto de dicha información, sobre la cual no debería existir una interferencia ilegítima por parte de terceros; asimismo, implica la posibilidad de que dentro de los límites que franquean la Constitución y la Ley, se tenga capacidad para ejercer cierto control sobre el uso que se haga de tal información, aunque el poseedor de la misma sea otra persona. Dichas dimensiones del derecho pueden ser perfectamente cumplidas si son aplicadas a una persona jurídica, por lo que no se advierte razones para negar la titularidad del mismo ni, en consecuencia, limitar su acceso al hábeas data, como mecanismo de tutela en sede de jurisdicción constitucional".

6.2.1.1.3 Sobre la naturaleza de la información personal de una persona jurídica

1	**Las personas jurídicas son titulares de los datos propios del ente social**	"Ante afirmaciones como las presentadas en esta sentencia cabe, sin embargo, realizar una aclaración importante, atinente a la noción de información "personal". Esta Corte considera imprescindible distinguir entre la información que atañe a la persona jurídica y aquella que puede ser considerada como de dominio de sus asociados, principalmente debido a que en aplicación errónea de la garantía del hábeas data, podría vulnerarse el derecho a la protección de datos e información personal de individuos que,

2	**La persona jurídica no es titular de los datos de sus miembros, socios o representantes**	aunque vinculados a la persona jurídica, no son identificables con ella. La tradicional noción del derecho civil, según la cual las personas jurídicas, así como los derechos y obligaciones de las que son titulares son distintos de los que la conforman, puede ser de utilidad para la diferenciación descrita. Si las personas jurídicas tienen el derecho a reclamar por medio del hábeas data actos tendientes a la protección de "... datos personales e informes (...) sobre sí misma, o sobre sus bienes...", este derecho solamente puede extenderse a sus socios, representantes legales y personas relacionadas, en tanto la posición que ocupan y la relación jurídica establecida respecto de la persona jurídica, y estrictamente respecto de ellas. No es dable, entonces, que una persona jurídica reclame como suyo el derecho a la protección de datos e información personal de quienes están relacionados con ella, en tanto este derecho solo corresponde a la persona a quien le es atinente, salvo que la exigencia de protección por parte de la persona jurídica se sustente en la debida autorización de sus socios o representantes legales".

6.2.1.1.4 Diferencia entre dato, archivo, documento, banco e información

1	**Se debe acudir a la doctrina para la diferenciación entre conceptos como "documento", "archivo", "dato", "banco de datos" e "información"**	"El problema respecto de la diferenciación entre conceptos como «documento», "«archivo», «dato», "banco de datos», «información» y otros relacionados con la materia, sin duda no es estrictamente jurídico, sino que corresponde también, entre otros campos, al de la informática. Empero, las implicaciones del sentido y alcance que se dé a cada uno de los conceptos enunciados, así como a la correcta diferenciación entre ellos, deberá ser determinado a través de un ejercicio hermenéutico, y por tanto, tendrá directa relación con el contenido del derecho constitucional protegido por medio de la acción de hábeas data. Así, para la solución del caso concreto y la emisión de reglas jurisprudenciales que se deriven de los hechos presentados, esta Corte deberá recurrir a las fuentes doctrinarias que permitan comprender qué protege la garantía jurisdiccional en particular".
2	**Dato e información son asimilables pero tienen diferencias respecto de su carácter informativo**	"En primer lugar, está el término «dato». Este es en su acepción técnica, de acuerdo con el Diccionario de la Real Academia Española: una "[i]nformación dispuesta de manera adecuada para su tratamiento por un ordenador". De acuerdo con dicha definición, los datos y la información serían conceptos asimilables, en tanto un dato sería la especie de información apta para ser procesada de diversas formas. Sin embargo, se ha identificado en la doctrina sobre la protección de datos una distinción entre los conceptos «dato» e «información» a la que se adscribe esta Corte, como lo relata Osvaldo Gonzaíni: Algunos entienden datos a la representación de hechos, conceptos o instrucciones bajo una forma adaptada a la comunicación, a la interpretación o al tratamiento por seres humanos o máquinas, y por informaciones al significado que toman los datos de acuerdo con convenciones vinculadas a éstos".
3	**Se protege el dato o la información no el medio por el**	"Hechas las distinciones anteriores, cabe señalar que tanto los datos como la información, son conceptos que giran en torno a la capacidad cognitiva atribuida en primera instancia al ser humano, así como a las máquinas como instrumento ordenado a la utilidad que el primero les dé. Al ser tales,

	cual se expresa, sea este un documento físico o electrónico	entonces, su expresión física por medio de determinadas señales dibujadas sobre un papel, o impulsos eléctricos, variaciones en las ondas, etc., denotan únicamente el medio por el cual se expresan, pero no pueden ser identificados con ellos. Así, si el dato es una representación de determinado fenómeno y la información es el significado de dicha representación adecuada a determinado fin en el proceso comunicativo, el «documento» funge como uno de varios medios en los que es posible impregnar o «imprimir" tal representación por medio de símbolos, a fin de lograr la preservación del dato y la información que se puede extraer de él. Por ende, no interesa para el hábeas data, como garantía, el papel y la tinta utilizados para registrar el dato, ni el disco duro en el cual se encuentre la información -denominados por el constituyente como «soporte material o electrónico» de los datos-, ni cualquier forma ideada por el ingenio humano para su preservación, sino que, como la expresión lo señala, el derecho tutelado recae sobre el dato mismo y el uso informativo que se le dé".
4	**Diferencia entre dato e información**	"Algunos entienden datos a la representación de hechos, conceptos o instrucciones bajo una forma adaptada a la comunicación, a la interpretación o al tratamiento por seres humanos o máquinas, y por informaciones al significado que toman los datos de acuerdo con convenciones vinculadas a estos". "El dato es difícil que, por sí solo, pueda tener una incidencia grande o grave en la llamada privacidad. Esto es, mientras el dato no resuelva una consulta determinada, no sirva a un fin, no dé respuestas o no oriente la posible solución a un problema, es el antecedente o punto de partida para la investigación de la verdad; pero, en el momento en que ese mismo dato da respuesta a una consulta determinada, o sirve a un fin, o se utiliza para orientar la solución de un problema, se ha convertido en información. Como conclusión, los datos están protegidos por medio de la garantía constitucional del *habeas data*, siempre que cumplan con una función informativa respecto de las personas y sus bienes y por ende, su comunicación, interpretación o tratamiento afecta en mayor o menor medida los derechos de aquel a quien se refieren".

La posición jurisprudencial referencial que limita la procedencia del *habeas data* a los datos informativos o con función informativa, debiera ser aplicada solo a los otros derechos protegidos por esta garantía jurisdiccional como: el honor, el buen nombre y la intimidad personal y familiar, en vista de que, en el caso del derecho a la protección de datos personales, el *habeas data* debe adaptarse al contenido de este derecho fundamental y resguardar no solo el dato con contenido informativo, sino también proteger al dato por sí solo, porque, aunque inicialmente carece de la característica informativa, puede ser tratado, perfilar a un individuo y afectar su autodeterminación informativa e incluso otros derechos fundamentales.

6.2.1.1.5 Sujetos pasivos

1	**Las autoridades de una persona jurídica no son sujetos pasivos del derecho a recibir quejas y peticiones**	"Respecto de la segunda vulneración alegada, cabe indicar que los integrantes de la directiva saliente de una compañía no pueden calificarse como «autoridades», en los términos utilizados por la Constitución de la República, sino como representantes legales, puesto que la «autoridad» a la que se refiere la Norma Suprema proviene del ejercicio de la potestad pública, o al menos del actuar por concesión o delegación de dicha potestad. Por lo tanto, no pueden ser considerados sujetos pasivos del derecho constitucional a dirigir quejas y peticiones y a recibir atención o respuesta, sin perjuicio de que figuras análogas estén establecidas en la legislación secundaria".

6.2.1.2 *Ratio decidenci:* efecto vinculante

A través de las sentencias No. 068-10-SEP-CC y No. 001-14-PJO-CC y la Corte Constitucional en ejercicio de sus atribuciones constitucionales conferidas en el artículo 436 numeral 1 y 6 de la CRE, procede a emitir precedente jurisprudencial obligatorio con efectos *erga omnes*, sobre *habeas data* y protección de datos personales, para lo cual emite las siguientes *ratio decidendi*:

6.2.1.2.1 Sentencia No. 068-10-SEP-CC, Corte Constitucional

1	**Las personas jurídicas son titulares de derechos fundamentales que les corresponden conforme su naturaleza social**	"En torno a esta apreciación realizada por la parte recurrida, esta Corte reitera que pese a que las personas jurídicas no sean titulares de todos los derechos constitucionales fundamentales, sí lo son de aquellos que les correspondan, según su naturaleza social y siempre en atención a la definición constitucional de los derechos de los que se trate, condición de la cual el Estado en sí no es ajeno y que, además, algunos de los derechos constitucionales fundamentales sólo son predicables de ciertas personas naturales, como es el caso de los derechos constitucionales fundamentales de los niños, el de la no extradición de numeral 7 Numeral 4 del artículo 44, de las Reglas de Procedimiento para el Ejercicio de las Competencias de la Corte Constitucional para el Período de Transición. (8 Guillermo Cabanellas de Torres, Diccionario Enciclopédico de Derecho)".[504]

6.2.1.2.2 Sentencia No. 001-14-PJO-CC, Corte Constitucional

[504] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 068-10-SEP-CC], en ROS, No. 372 (27 de enero de 2011).

1	**Se analizará en cada caso si la persona jurídica es titular de un derecho fundamental**	"La determinación respecto de si una persona jurídica puede beneficiarse de una provisión constitucional que contenga un derecho constitucional debe hacerse caso por caso, en consideración de las posibilidades derivadas de su naturaleza social, así como de los términos en los que está formulado el derecho en la Norma Constitucional".[505]
2	**La autodeterminación informativa es parte del derecho a la protección de datos personales**	"En el caso de la autodeterminación informativa, como parte del derecho a la protección de datos personales, implica la necesidad de garantizar la protección de la esfera íntima de las personas, así como la posibilidad de ejercer control sobre los datos personales del sujeto, aunque no se encuentren en su poder".[506]

[505] Ibíd., [Sentencia No. 001-14-PJO-CC], en ROS, No. 281 (2 de julio de 2014).
[506] Ibíd.

3	**Las personas jurídicas por las características del derecho pueden ser titulares de la protección de datos personales**	"Por las características del derecho a la protección de datos personales, no se considera constitucionalmente adecuada la limitación a la calidad de las personas jurídicas como titulares del mismo; sin embargo, la información personal de dichos sujetos únicamente se extiende a las personas asociadas o a sus representantes legales, en tanto a la calidad que ostentan respecto de la persona jurídica, con estricto respeto al derecho a la protección de los datos personales y derechos conexos que le son atinentes a su naturaleza".[507]
4	**Legitimado activo debe ser el titular del derecho a la protección de datos personales**	"La legitimación activa para la presentación de la acción de hábeas data requerirá que quien lo haga sea el titular del derecho a la protección de datos personales que se alegue vulnerada, o su representante legitimado para el efecto".[508]
5	**Acreditada la representación de la persona jurídica no procede excepción de falta de legitimación**	"Para acreditar la representación de las personas jurídicas será suficiente la entrega del documento que la ley que regule la materia determine como suficiente para considerar iniciadas sus funciones como representante. El juez constitucional, una vez acreditada la representación, deberá tramitar la acción sin que medie excepción sobre el cumplimiento de los requisitos de ley respecto del documento entregado, lo que deberá ser dilucidado por los organismos competentes en sede ordinaria".[509]
6	**El *habeas data* no puede invocarse para requerir la entrega física de los documentos que contienen información personal**	"El hábeas data, como mecanismo de garantía del derecho a la protección de datos personales, no podrá ser incoado como medio para requerir la entrega física del soporte material o electrónico de los documentos en los que se alegue está contenida la información personal del titular sino para conocer su existencia, tener acceso a él y ejercer los actos previstos en el artículo 92 de la Constitución de la República; el juez está obligado a utilizar todos los mecanismos que establece la ley para efectos de garantizar debida y eficazmente los actos constantes en el artículo referido".[510]

Si bien esta sentencia reconoce por primera vez a la autodeterminación informativa como uno de los elementos esenciales del derecho a la protección de datos personales en Ecuador, sin embargo, no desarrolla con la profundidad necesaria este tema, ya que la *ratio decidendi* termina refiriéndose a la calificación de la legitimación activa de las personas jurídicas para presentar acciones de *habeas data* dependiendo de cada caso.

Ahora bien, es destacable que dicha resolución determine que la autodeterminación informativa garantiza, tanto la protección de la esfera íntima de las personas, como del acceso y la decisión sobre los datos personales del sujeto. Una interpretación progresiva y que garantice la efectiva vigencia de estos derechos sería la de entender a este pronunciamiento constitucional como una visibilización de la autodeterminación informativa como elemento sustancial, tanto del derecho a la intimidad como del derecho a la protección de datos personales.

[507] Ibíd.
[508] Ibíd.
[509] Ibíd.
[510] Ibíd., Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 048-16-SIS-CC], ROS No. 878 (10 de noviembre de 2016); Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 138-16-SEP-CC], ROS No. 799 (18 de julio de 2016).

Finalmente, mediante la cita de autores, se analiza la complejidad del derecho a la protección de datos personales, ya que su contenido conjuga derechos como el de la autodeterminación informativa, así como el de acceso a la información o datos personales, el de información de la finalidad de su recogida y, además, principios rectores que lo materializan y garantías que permiten su efectiva vigencia y tutela.

6.2.2 Interpretación con carácter vinculante los tratados internacionales de derechos humanos con efectos *erga omnes:*

El numeral 1 del artículo 436 de la CRE, establece entre las atribuciones de la Corte Constitucional la relativa a la interpretación de carácter vinculante, esto es "conforme y condicionada con efectos erga omnes"[511], de los tratados internacionales de derechos humanos ratificados por el Estado ecuatoriano, a través de sus dictámenes y sentencias.

La Corte Constitucional, respecto del efecto vinculante, aclara que la interpretación realizada por la Corte Constitucional es:

> […] de obligatorio acatamiento, razón por la cual, en caso de desconocimiento de estas interpretaciones, se estará a lo dispuesto en la Constitución de la República, la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional y el Reglamento de Sustanciación de Procesos de Competencia de la Corte Constitucional.[512]

En el período comprendido desde 2008 hasta 2019, fecha de corte de esta investigación, solo existe una sentencia relativa a la temática de protección de datos personales y *habeas data* dictada por la Corte Constitucional en el ejercicio de la facultad de interpretar con carácter vinculante los tratados internacionales de derechos humanos.

La sentencia en cuestión, invoca el artículo 436 numerales 1 y 3 de la Constitución de la República como atribuciones que permiten a la Corte Constitucional efectuar:

> […] interpretación conforme y condicionada con efectos *erga omnes* del artículo 50 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional […] Con el fin de evitar que en la tramitación de las acciones de hábeas data se produzcan vulneraciones a los derechos protegidos por esta acción o abusos en la utilización de la garantía por parte de los usuarios de la administración de la justicia constitucional.[513]

Esta sentencia es la No. 00182-15-SEP-CC, dictada por la Corte Constitucional del Ecuador, cuyo contenido se analizará a continuación. Para el respectivo análisis de la sentencia se revisarán los pronunciamientos meramente orientativos: *obiter dicta*, y los criterios vinculantes o *ratio decidenci.*

6.2.2.1 *Obiter dicta:* efecto meramente referencial

La parte considerativa de las sentencias constitucionales constituyen únicamente criterios orientativos para jueces y tribunales de inferior nivel. A continuación, constan el análisis de la resolución No. 00182-15-SEP-CC, para lo cual se ha organizado los *obiter dicta* por temas y subtemas bajo los criterios que constan a continuación.

---

[511] CORTE CONSTITUCIONAL, [Sentencia No. 00182-15-SEP-CC].
[512] Ibíd.
[513] Ibíd.

6.2.2.1 Sobre la naturaleza jurídica de la garantía constitucional de *habeas data*

1	**El *habeas data* es una garantía jurisdiccional que tiene su origen en la protección de datos personales**	"Es necesario precisar que el hábeas data es una garantía jurisdiccional que tiene su origen en el principio contenido en el artículo 66 numeral 19 de la Constitución, mismo que prescribe que el Estado reconoce y garantiza a todas las personas el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección".
2	**El *habeas data* es la acción que materializa las diversas manifestaciones del derecho de petición para la operatividad de las garantías jurisdiccionales**	"Ahora bien, de conformidad con la normativa contenida en los artículos 92 de la Constitución de la República del Ecuador y 49, 50 y 51 de la Ley Orgánica de Garantías jurisdiccionales y Control Constitucional, la figura constitucional del hábeas data constituye una acción en virtud de la que materializan las diversas manifestaciones del derecho de petición consagrado constitucionalmente y requerido para la operatividad de las garantías jurisdiccionales, una garantía que le permite a una persona concurrir al órgano jurisdiccional a fin de que sus derechos sean protegidos; goza de carácter autónomo, por cuanto, posee un perfil propio regulado tanto en la Constitución como en la ley de la materia y tutela datos o información inherente a una persona, a fin de salvaguardar su derecho a la intimidad personal y familiar".
3	**El *habeas data* goza de carácter autónomo, posee un perfil propio pues tutela datos o información inherente a una persona, a fin de salvaguardar su derecho a la intimidad personal y familiar**	
4	**La acción de *habeas data* es la garantía constitucional, a efectos de salvaguardar el derecho a la intimidad personal y familiar**	"Por consiguiente, la acción de hábeas data es la garantía constitucional que le permite a la persona natural o jurídica, acceder a la información que sobre sí misma reposa en un registro o banco de datos de carácter público o privado a fin de conocer el contenido de la misma y de ser el caso, exigir su actualización, rectificación, eliminación o anulación cuando aquella información le causa algún tipo de perjuicio a efectos de salvaguardar su derecho a la intimidad personal y familiar".
5	**La acción de *habeas data* protege el derecho al honor, a la buena reputación, a la buena imagen, a la intimidad personal y familiar**	"Contenido de la acción constitucional de hábeas data De la lectura del artículo 92 del texto constitucional podemos extraer el contenido de la acción de hábeas data, en especial, cobra importancia los derechos que esta garantía jurisdiccional protege, siendo estos el derecho al honor, a la buena reputación, a la buena imagen, a la intimidad personal y familiar".

6	**El *habeas data*, tiene como función garantizar el derecho de las personas a la protección de sus datos de índole personal, a través del acceso, decisión respecto de su utilización, rectificación, anulación o su eliminación**	"En el caso de la acción constitucional de hábeas data, en atención a su naturaleza, contenido y alcance -conforme a la explicación ut supra- tiene como función garantizar el derecho de las personas a la protección de sus datos de índole personal a través del acceso, decisión respecto de su utilización, rectificación, anulación o su eliminación".
7	**El *habeas data* protege el derecho a la intimidad de la persona, pues su información no tiene carácter de pública y no puede divulgarse en forma libre**	"En consecuencia, la acción constitucional de hábeas data en el fondo lo que pretende es proteger el derecho a la intimidad de la persona, puesto que no toda la información relativa a esta tiene el carácter de pública y por tanto, de divulgable en forma libre.".
8	**El ámbito de aplicación de la acción constitucional del *habeas data*, posee una órbita específica, esto es, la información íntima de una persona**	"El ámbito de aplicación de la acción constitucional del hábeas data, posee una órbita específica, esto es, la información íntima de una persona, la cual puede estar contenida en diversas formas, tales como documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí o sobre sus bienes, repose en custodia de personas naturales o jurídicas públicas o privadas, ya sea en soporte material o electrónico".

6.2.2.2 Sobre la naturaleza jurídica de los derechos de acceso y decisión de los datos personales a través del *habeas data*

1	**El *habeas data*, se caracteriza por otorgarle el derecho al titular de la información, que reposa en una base de datos, bajo custodia de una persona natural o jurídica pública o privada, de solicitar su actualización, rectificación o corrección, eliminación o anulación.**	"Del fragmento de sentencia que precede se colige que mediante ella, esta Corte ha sido muy precisa en determinar el ámbito de aplicación de la garantía jurisdiccional de hábeas data, para lo cual ha desarrollado cada una de las posibilidades que daría lugar a la activación de dicha acción. En aquel sentido, ha determinado que la facultad que tiene la persona para acceder a la información que sobre ella reposa en una base de datos -bajo custodia de una persona natural o jurídica pública o privada, es la que caracteriza el hábeas data, la que justifica su existencia y en virtud de la cual le es posible, a la persona titular de dicha información, solicitar su actualización, rectificación o corrección, eliminación o anulación".
2	**El titular tendrá derecho a conocer el uso, la finalidad, el origen, destino y tiempo de vigencia de su información personal.**	"En virtud de ello, dicha persona tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de su información personal y el tiempo de vigencia del archivo o banco de datos".

3	**El acceso y conocimiento permite a su vez al titular solicitar actualización, rectificación eliminación o anulación de los datos personales.**	"Para el efecto, la persona titular de los datos podrá solicitar al responsable el acceso sin costo a la información a fin de conocer su contenido, lo cual, a su vez, le permitirá solicitar su actualización, rectificación, eliminación o anulación".
4	**El derecho de acceso se podrá solicitar al responsable sin costo para el titular.**	

6.2.2.3 Sobre la procedibilidad del *habeas data*

1	**La pretensión básica o esencial del hábeas data debe estar dirigida, únicamente a solicitar información personal.**	"Para ello, la pretensión básica o esencial del hábeas data debe estar dirigida, únicamente a solicitar información personal, la cual deberá ser recibida o entregada por la persona natural o jurídica pública o privada que la posea, dentro de un plazo razonable, circunstancias que configuran el derecho de acceder a la información personal; evento que se hace efectivo cuando se recibe clara, total y oportunamente todo aquello que se busca".
2	**El *habeas data* se hace efectivo cuando se recibe clara, total y oportunamente todo aquello que se busca, dentro de un plazo razonable**	
3	**La información personal reposa en soporte material o electrónico en registros de personas naturales o jurídicas públicas o privadas.**	"El contenido de lo que respecta a la información personal se refiere a aquélla que reposa en soporte material o electrónico en registros de personas naturales o jurídicas públicas o privadas".
4	**El elemento constitutivo para la vulneración del derecho de acceso y el derecho de decisión de los datos personales se produce cuando la persona natural o jurídica pública o privada niega la solicitud de *habeas data*.**	"De esta manera se evidencia que el elemento constitutivo para la vulneración del derecho de acceso y el derecho de decisión de los datos personales se produce cuando la persona natural o jurídica pública o privada niega la solicitud que el titular de la información efectúa en ejercicio de su derecho constitucional, lo cual permite al afectado incoar la acción constitucional".
		"Salvo el caso del derecho de utilización que implica el manejo que la persona o entidad depositaria de la información da a esta, las vulneraciones a los derechos de acceso y de decisión se producen por la negación del depositario de la información de atender la solicitud efectuada por el titular. Dicha denegatoria puede efectuarse de manera expresa, a través de una actuación inequívoca de quien tiene la administración del soporte en el que reposan los datos del solicitante".
5	**La falta de respuesta de las entidades que tienen a cargo datos personales**	"Por otra parte, la falta de respuesta de las entidades que tienen a cargo la gestión de datos personales

	frente a la solicitud de *habeas data* genera una situación de incertidumbre e inseguridad jurídica.	frente a la solicitud que en este sentido es efectuada por los titulares del derecho constitucional contenido en el artículo 66 numeral 19 de la Norma Fundamental impide a estos el ejercicio pleno del derecho en comento, generando una situación de incertidumbre e inseguridad".
6	**La ausencia de respuesta de la entidad que tenga a cargo la información personal debe ser tomada como negativa y por ende, procede el hábeas data.**	"En virtud de lo dispuesto en el artículo 86 numeral 2 literal a de la Constitución de la República, que establece que los procedimientos de las garantías jurisdiccionales deben ser rápidos, sencillos y eficaces; la ausencia de respuesta de la entidad que tenga a cargo la administración de los datos de una persona respecto de la solicitud de un titular de esta información debe ser tomada como negativa y por ende, se enmarcaría en los supuestos del ámbito de procedencia de esta garantía jurisdiccional con la finalidad de que la garantía de hábeas data pueda activarse de manera eficaz, optimizando el contenido del derecho que esta tutela".

6.2.2.4 Sobre autodeterminación informativa:

1	**La autodeterminación informativa tiene como finalidad proteger otros derechos constitucionales que podrían verse afectados cuando se utilizan datos personales.**	"<<El derecho a la protección de datos>> y específicamente, su elemento denominado "autodeterminación informativa-" tiene como finalidad proteger otros derechos constitucionales que podrían verse afectados cuando se utilizan datos personales, tales como la intimidad, la honra, la integridad psicológica, entre otros".

6.2.2.5 Sobre *habeas data* y debido proceso

1	**La petición de acceso, decisión o utilización de los datos personales implica la existencia de un proceso, administrativo o privado, en el que se resuelve o determina sobre los derechos y obligaciones de una persona, por lo que este se encuentra regido por las normas del debido proceso.**	"De esta forma se puede evidenciar que la procedibilidad del hábeas data[MV2] depende de la decisión que adopta una autoridad pública o privada respecto de la petición que efectúa el titular respecto de su derecho consagrado en el artículo 66 numeral 19 de la Constitución de la República. Así las cosas, es importante determinar que la petición de acceso, decisión o utilización de los datos personales implica la existencia de un proceso (en este caso administrativo o privado) en el que se resuelve o determina sobre los derechos y obligaciones de una persona, por lo que este se encuentra regido por las normas del debido proceso que se encuentran

		previstas en el artículo 76 de la Constitución".
2	**Las personas públicas o privadas que tengan a cargo la información personal ante las solicitudes de *habeas data* deberán pronunciarse motivadamente atendiendo a los principios de inmediación y celeridad.**	"Por este motivo, es imprescindible que las autoridades públicas o privadas que administren información protegida por el artículo 66 numeral 1921 de la Norma Fundamental, respetando las garantías de las personas se pronuncien motivadamente respecto de las peticiones que en este sentido efectúen los titulares de la información que se encuentra bajo su gestión. Es por esta razón que las personas y entidades que tienen a su cargo datos personales deben responder a las solicitudes que sobre estos realicen los titulares de esta información. Esta respuesta debe atender a los principios de inmediación, celeridad y debe estar motivada suficientemente, de conformidad con la Constitución y la ley".

6.2.2.2 *Ratio decidenci:* efecto vinculante en virtud de los numerales 1 y 3 del artículo 436 de la Constitución

A través de la sentencia No. 00182-15-SEP-CC, la Corte Constitucional en ejercicio de sus atribuciones Constitucionales conferidas en el artículo 436 numerales 1 y 3 de la Constitución de la República, procede a interpretar condicionadamente y con efectos *erga omnes* el artículo 50 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, para lo cual emite las siguientes *ratio decidendi*:

1	**La entidad a quien se requiere el *habeas data* responderá la solicitud efectuada por el titular de la información personal en un plazo razonable**	"La persona natural o jurídica pública o privada requerida deberá responder a la solicitud efectuada por el titular de la información personal en un plazo razonable que permita de mejor manera la satisfacción del derecho, que dependerá de la cantidad de la información requerida, del tipo de pedido y de la propia conducta de la persona natural o jurídica pública o privada que posea la administración de los datos requeridos".
2	**Los criterios que permiten determinar el plazo razonable son: cantidad de información, tipo de pedido, conducta de la entidad a cargo de los datos personales**	
3	**Calificación de la razonabilidad deberá realizarla el juez**	"La calificación de la razonabilidad de este plazo deberá ser realizada por el juez competente en la acción de Hábeas Data, al momento de la calificación de la demanda de esta garantía jurisdiccional".
4	**La falta de contestación de la entidad a cargo de los datos**	"La falta de contestación de la persona natural o jurídica pública o privada que tenga bajo su administración los

	personales se considera negativa tácita a la solicitud de acceso presentado por el titular y habilita presentar *habeas data*	datos de una persona, sobre la solicitud que su titular efectúe respecto del acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes en poder de éstas, o respecto de la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten los derechos de estos titulares, será considerada como negativa tácita por lo que se enmarcará en los presupuestos de la acción de Hábeas Data contenidos en los numerales 1 y 2 del artículo 50 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional".

6.2.2.3 *Ratio decidenci*: efecto vinculante en virtud de los numerales 1 y 6 del artículo 436 de la Constitución

En la citada sentencia No. 00182-15-SEP-CC, la Corte Constitucional en ejercicio de sus atribuciones Constitucionales conferidas en el artículo 436 numerales 1 y 6 de la Constitución de la República, procede a dictar precedente jurisprudencial obligatorio, para lo cual emite las siguientes *ratio decidendi*:

1	**Respecto de la naturaleza de la acción de *habeas data***	"La acción de hábeas data es la garantía constitucional que le permite a la persona natural o jurídica, acceder a la información que sobre sí misma reposa en un registro o banco de datos de carácter público o privado, a fin de conocer el contenido de la misma y de ser el caso, exigir su actualización, rectificación, eliminación o anulación cuando aquella información le causan algún tipo de perjuicio, a efectos de salvaguardar su derecho a la intimidad personal y familiar".
2	**Contenido: El hábeas data, protegerá el derecho a la intimidad, la honra, la integridad psicológica de la persona**	"Contenido: La acción constitucional de hábeas data, protegerá el derecho a la intimidad, la honra, la integridad psicológica de la persona, puesto que no toda la información relativa a estos tiene el carácter de pública y por tanto de divulgable en forma libre. En efecto, existen asuntos relativos a su familia, sus creencias religiosas y espirituales, su filiación política, su orientación sexual, entre otras, que en caso de ser divulgadas de forma inadecuada e inoportuna podrían ocasionarle serios perjuicios en la esfera personal".
3	**Contenido: Existen asuntos relativos a la familia, creencias religiosas o espirituales, filiación política, orientación sexual, que en caso de ser divulgadas de forma inadecuada e inoportuna podrían ocasionar serios perjuicios en la esfera personal**	
4	**Alcance: el titular debe plantear su pretensión conforme la Ley y jurisprudencia sobre *habeas data* para no desnaturalizarla y agilitar la administración de**	"Alcance: La acción constitucional de hábeas data tiene lineamientos específicos que deben ser observados por quien ejerce la legitimación activa de la misma, quien de forma especial, al redactar su pretensión deberá estructurar su pedido de conformidad con los parámetros establecidos

	justicia	para el efecto en la Constitución, en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional y en la jurisprudencia vinculante emitida por este Organismo sobre dicha acción lo cual coadyuvará, en primer lugar a que la acción en comento no se desnaturalice y en segundo lugar, a que la administración de justicia constitucional sea más ágil y eficaz para el fin que se persigue".
5	**Interpretación vinculante**	"La interpretación conforme del artículo 50 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional realizada por la Corte Constitucional en esta sentencia, es de obligatorio acatamiento, razón por la cual, en caso de desconocimiento de estas interpretaciones, se estará a lo dispuesto en la Constitución de la República, la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional y el Reglamento de Sustanciación de Procesos de Competencia de la Corte Constitucional".

Del análisis comparativo del contenido de las sentencias vinculantes emitidas luego de la Constitución de 2008, estas son: la sentencia No. 001-14-PJO-CC y sentencia No. 00182-15-SEP-CC se concluye que su contenido es complementario, incluso se mantienen y desarrollan varios temas en sentido similar y evolutivo. Ya que, en la primera sentencia se reconoce a la autodeterminación informativa como parte del contenido esencial del derecho a la protección de datos personales y en la segunda resolución, se la considera también como parte sustancial del *habeas data*.

En conjunto configuran elementos que permiten realizar avances importantes en la clarificación y aplicabilidad de esta garantía constitucional. Tal como ocurre con los siguientes criterios vinculantes: a) reconocimiento como titulares del derecho a la protección de datos y como legitimado activo a las personas jurídicas, bajo condiciones específicas; b) definiciones sobre datos, información, archivo, documento, banco e información; c) naturaleza jurídica del *habeas data*, caracterizada por otorgar al titular de la información, que reposa en una base de datos, bajo custodia de una persona natural o jurídica pública o privada, el derecho de solicitar su actualización, rectificación o corrección, eliminación o anulación; d) determinación de condiciones para la procedibilidad del *habeas data* como: la determinación de un plazo razonable para contestar ante la solicitud de acceso de un titular de datos; e) la calificación de la razonabilidad por parte del juez del *habeas data*; f) la determinación de que la falta de contestación de la entidad a cargo de los datos personales se considera negativa tácita a la solicitud de acceso presentado por el titular y habilita presentar *habeas data*.

Ahora bien, existen dos temas que deben ser interpretados desde una perspectiva progresiva de derechos.

Si bien en la sentencia No. 001-14-PJO-CC se reconoce que el *habeas data* tiene su origen en el derecho a la protección de datos personales, al tenor de la cita que se transcribe:

> Es necesario precisar que el hábeas data es una garantía jurisdiccional que tiene su origen en el principio contenido en el artículo 66 numeral 19 de la Constitución, mismo que prescribe que el Estado reconoce y garantiza a todas las personas el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento,

> distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.[514]

Sin embargo, en la sentencia No. 00182-15-SEP-CC señala que "La acción constitucional de hábeas data, protegerá el derecho a la intimidad, la honra, la integridad psicológica de la persona", pero no menciona el derecho a la protección de datos personales, así como tampoco a la imagen y la propia voz, el derecho a la identidad o a la rectificación en medios de comunicación, que son otros derechos que también han sido reconocidos en resoluciones no vinculantes como cobijados por esta garantía constitucional.

En sentencia No. 0002-14-HD que precisamente cita para su análisis la resolución No. 00182-15-SEP-CC previamente estudiada, señala que es "necesario resaltar también que hay que distinguir, que la información a la que se pretende acceder, es aquella que se vincula directamente con los derechos constitucionales de la personalidad, motivo por lo que, se tiene que excluir la información que por su naturaleza no afecta prima facie estos derechos constitucionales".[515] Respecto de quien debe verificar, caso a caso, la naturaleza o tipo de dato al que se quiere acceder a través de la garantía constitucional, se estará a lo dispuesto en la siguiente resolución:

> […] la responsabilidad de determinar si la información a la que se pretende acceder, mediante la garantía jurisdiccional de hábeas data, tiene relación directa con los derechos constitucionales de la personalidad, le corresponde, en exclusiva, al juez constitucional, en calidad de actor protagónico en el respeto a la Constitución de la República.[516]

La incorporación de otros derechos de la personalidad resulta lógica, incluso del análisis de los *obiter dicta* de las dos sentencias revisadas, dado que los datos personales son las personas mismas en entornos digitales, manifestación misma de su existencia. Por lo que, todos aquellos derechos de la personalidad que a través de los datos personales se materializan a través de las TIC deberán ser tutelados por esta garantía jurisdiccional.

Se entiende por derechos de la personalidad:

> […] el conjunto de manifestaciones físicas y psíquicas del ser humano, derivadas de su individualidad, su modo de ser, que lo distinguen de otros seres humanos, haciéndolo un ser único e irrepetible. La Personalidad se encuentra protegida a través de los llamados derechos de la personalidad. Estos derechos tienen como finalidad la tutela de la dignidad humana, buscan otorgar un marco jurídico que proteja el libre desenvolvimiento de la personalidad humana.[517]

En consecuencia, es suficiente que los datos personales pongan en riesgo a la dignidad humana o impidan el libre desarrollo de la personalidad de su titular para que el *habeas data* proceda.

De lo dicho, el *obiter dicta* de la sentencia No. 00182-15-SEP-CC que determina que "el ámbito de aplicación de la acción constitucional del hábeas data, posee una órbita específica, esto es, la información íntima de una persona" debe ser interpretado de forma progresiva.

---

[514] CORTE CONSTITUCIONAL, [Sentencia No. 00182-15-SEP-CC].
[515] Ibíd., [Sentencia No. 00182-15-SEP-CC]; [Sentencia No. 0002-14-HD] en ROEC, No. 2 (5 de junio de 2017)
[516] Ibíd., Sentencia No. 175-14-SEP-CC] en ROEC, No. 406 (30 de diciembre de 2014) ; [Sentencia No. 0002-14-HD] en ROEC, No. 2 (5 de junio de 2017)
[517] E. DE LA PARRA TRUJILLO, "Los derechos de la personalidad: Teoría General y su distinción con los derechos humanos y las garantías individuales", *Jurídica. Anuario del Departamento de Derecho de la Universidad Iberoamericana*, No. 31 (2001): 141.

Toda vez que una interpretación restrictiva de este texto, configura un *habeas data* acotado a datos íntimos, que impediría el ejercicio de la autodeterminación informativa, pues este contenido esencial se debe aplicar a cualquier tipo de dato con la sola condición de que sea personal. No es necesaria la condición de íntimo, esto es del fuero personal o familiar, o de categorías especiales de datos como aquellos denominados sensibles, esto es, alusivos a sus creencias y orientaciones, por ejemplo.

Nuevamente, la interpretación progresiva de derechos es considerar que esta afirmación se aplica únicamente a aquellos *habeas data* que hayan sido incoados con la intimidad como supuesto de derecho vulnerado. Ya que, si son otros los derechos en discusión, como son la imagen y la voz, la identidad, y la protección de datos personales, entre otros, para que la garantía constitucional proceda no es condicionante necesaria que los datos sean íntimos.

Adicionalmente, conforme ha señalado la doctrina y de la simple lectura del artículo 66 tanto en sus numerales 19 y 20 de la CRE se colige que la intimidad y la protección de datos personales se han separado como derecho. La finalidad del derecho a la protección de datos personales, con configuración autónoma e independiente de la intimidad, es darle a la persona titular el poder de decidir sobre sus datos, la autodeterminación sobre cualquier tipo de dato personal, no solo sobre los íntimos sino incluso los inocuos o superficiales.

Porque a través de los datos irrelevantes se pueden construir perfiles completos de personalidad que inclusive pueden ser predictivos, por lo que este conjunto de datos pueden ser aún más invasivos que los datos íntimos, pues no solo pueden afectarse a las personas a través de la difusión de datos íntimos, sino que se puede afectar la voluntad de las personas o asignarse de forma equivocada categorías o valoraciones injustas, incorrectas o discriminatorias.

6.2.3 Consulta de norma con carácter vinculante:

Conforme los artículos 429 y 436 numeral 1 de la CRE, y del artículo 76 numeral 5 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, la Corte Constitucional a través de Sentencia No. 006-17-SCN-CC, que tiene efecto vinculante, ha realizado interpretación conforme y condicionada de la normativa contenida en el Título II, Capítulo II del Código Orgánico General de Procesos.

En tal sentido, la citada resolución señala que, para procesos de garantías jurisdiccionales de acción de protección, acceso a la información pública y acción de *habeas data*, se debe aplicar exclusivamente de forma supletoria, el Capítulo III Sobre Excusa y Recusación del Código General de Procesos.

En especial, el artículo 22, relativo a las causas de excusa o recusación; el artículo 23, sobre el plazo de presentación de dos días término por parte del juzgador y de recusación en caso de que este último no lo hiciere; el artículo 24, relativo a las causas de inadmisión de la recusación; artículo 25, sobre la subrogación de la o el juzgador que se ha excusado o recusado; artículo 26, sobre la competencia; artículo 27, alusivo a la caución; y el artículo 28, relativo a la audiencia.[518]

6.2.4 Resoluciones sobre protección de datos personales y *habeas data* posteriores a la Constitución de 2008 que no constituyen precedente obligatorio:

Los artículos 94 y 437 de la CRE, determinan que el Pleno de la Corte Constitucional es competente para conocer y resolver sobre las acciones extraordinarias de protección en contra de sentencias, autos definitivos y resoluciones con fuerza de sentencia que se encuentren firmes o ejecutoriados y que en el juzgamiento se haya violado, por acción u omisión, el debido proceso u otros derechos reconocidos en la Constitución.

Así mismo, el artículo 436 numeral 9 de la CRE determina la competencia de la Corte constitucional para conocer y sancionar el incumplimiento de las sentencias y dictámenes constitucionales.

Las decisiones tomadas en virtud de las competencias mencionadas son meramente orientativas pues tienen por objetivo reparar los errores de motivación y de transgresión de derechos de las decisiones de inferiores niveles.

A continuación las principales referencias jurisprudenciales sobre protección de datos personales y *habeas data*:

6.2.3.1 *Habeas data* no se trata de una acción procesal civil, sino de una garantía constitucional

[518] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 006-17-SCN-CC], en ROEC, No. 22 (05 de diciembre de 2017).

La necesidad de distinguir la naturaleza del *habeas data* como garantía constitucional diferenciándola de una acción procesal civil, radica en el abuso que las partes pueden hacer respecto de esta garantía, ya que como hemos revisado, pretende ser usada para realizar diligencias previas como exhibiciones de documentos, confesión judicial[519] u obtención de pruebas. Produciéndose perniciosas confusiones, situaciones que desnaturalizan el contenido de esta garantía tal como se señala en la sentencia que a continuación se transcribe:

> Si no se analiza este objetivo básico de la garantía constitucional del hábeas data, se presenta, como de hecho se da, una perniciosa confusión entre el hábeas data y la institución jurídica de la "exhibición", figura típica del procedimiento civil. (…) En el hábeas data no se obtienen pruebas, se accede a la información, se verifica la exactitud de la información del que la posee, se verifica qué uso está dando el poseedor a dicha información, se le impide que la difunda si ésta es errada, se cambia la información si es equivocada y se difundiría la verdadera información entre aquellos a quienes se emitió inicialmente, con el propósito de garantizar eficazmente los derechos constitucionales vinculados al honor, a la intimidad y a la buena fama. Así concebido y entendido el hábeas data, no se trata de una acción procesal civil, sino de una garantía constitucional con objetivos muy precisos, que busca que el accionante sepa: 1) Cuáles son los motivos legales por los que el poseedor de la información llegó a ser tenedor de la misma; 2) Desde cuándo tiene la información; 3) Qué uso se ha dado a esa información y qué se hará con ella en el futuro; 4) Conocer a qué personas naturales o jurídicas, el poseedor de la información hizo llegar la misma; por qué motivo, con qué propósito y la fecha en la que circuló la información; 5) Qué tecnología usa para almacenar la información; y, 6) Qué seguridades ofrece el tenedor de la información para precautelar que la misma no sea usada indebidamente[520].

6.2.3.2 La entidad a cargo de la información no está obligada a entregar información que no tiene y tampoco a generar la inexistente

En resolución sobre incumplimiento de sentencia de *habeas data*, la Corte niega el petitorio, por cuanto realiza un análisis similar al anterior. Ya que, en el peritaje realizado en la acción de *habeas data* primigenia, el perito designado, emitió un informe en el que asegura que no ha podido verificar o constatar la existencia de ciertos documentos. La Corte Constitucional actual, en resolución que no tiene efecto vinculante, pero que es orientadora de criterio, considera que, en este caso, el Banco no está en la obligación de generar dicha información, tal como señala a continuación:

> (…) En el caso in examine, una vez cumplido este procedimiento solemne, sobre la base del informe del perito, el juez determinó que en los archivos del Banco no existe el documento cuya entrega se reclama. Debido a esta circunstancia, no se puede exigir al accionado que lo reproduzca, pues a través de la acción de hábeas data, únicamente se puede exhibir lo que se tiene o posee realmente (…) este Organismo ratifica que la entrega del documento consistente en "el desglose de las acreditaciones a la obligación crediticia No. DAF-801796", es inejecutable, debido a que, como se constató de las diligencias procesales que dispuso y ejecutó el juez de instancia, este documento no existe en los archivos de la entidad demandada, por lo que el Banco no está en la obligación de generarla[521].

---

[519] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0022-2008-HD], en ROS, No. 133 (10 de julio de 2009).
[520] [Sentencia No. 019-09-SEP-CC2], en ROS, No.018 (3 de septiembre de 2009).
[521] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 007-15-SIS-CC], en ROS, No. 472 (02 de abril de 2015)

6.2.3.3 Derechos y facultades del *habeas data*

Dentro de los derechos y facultades del *habeas data* se encuentra el de conserva la información personal, por parte de quien sea el responsable de esta. Así como también, el de solicitar, al momento, el acceso a dicha información, su finalidad y destino, para ejercer los derechos de acceso, rectificación y anulación, tal como consta en la cita a continuación:

> De modo que la acción de hábeas data, obliga a toda entidad pública o privada, que conserva la información y documentación de las personas, a presentarla en el momento en que se lo requiera; asimismo, explicar y hacer conocer la finalidad, propósito, origen y destino de la documentación que reposa en sus archivos y banco de datos, cumpliendo de esta forma la obligación que tienen de garantizar el derecho de acceso, conocimiento y el derecho a la actualización, rectificación, eliminación o anulación de datos de las personas.[522]

De la transcripción que antecede, llama la atención la precisión que hace la Corte Constitucional respecto del derecho de las personas de acceder a información en el momento que se requiera y por ende la obligación del responsable de presentarla con esa misma oportunidad. De otro lado, en los derechos propios del *habeas data* no se enlista el de oposición. Situación que no significa que el derecho no está consagrado en el Ecuador, ya que el derecho de oposición es parte del contenido del derecho a la autodeterminación informativa, por el cual el titular tiene entre sus prerrogativas la de abstenerse a entregar información o de revocar el consentimiento de aquella que ya no desea mantener en manos de un determinado responsable.

En otra resolución, se aclara que el *habeas data* permite proteger derechos de una persona de la siguiente manera:

> [...] 1. Conociendo la existencia y la veracidad de la información personal o familiar solicitada. 2. Permitiendo el acceso a la información personal y familiar y conociendo el origen, uso, destino y tiempo de vigencia de la información solicitada. 3. Garantizando la actualización, rectificación o eliminación de la información solicitada; y 4. Garantizando la confidencialidad de la información al permitir determinar qué información puede ser difundida y qué información no debe ser difundida.[523]

El objetivo de esta garantía constitucional como señala la sentencia que se transcribe a continuación es tutelar o garantizar derechos de las personas, tales como: el derecho a dirigir peticiones y a recibir atención a las mismas:

> Lo anotado nos llevaría a afirmar que el hábeas data, al igual que el amparo, son mecanismos procesales constitucionales que procuran de manera ágil y sumaria garantizar el reconocimiento de los derechos de las personas físicas o naturales. La pretensión de la recurrente de requerir a través de esta garantía que la Municipalidad de Naranjal proceda a efectuar la entrega de copia de los planos de terrenos de su propiedad, tiene como propósito el que pueda ejercer su derecho a la defensa o demandar por el respeto a su derecho de propiedad, por tanto, si esta es la pretensión de la recurrente, no podemos soslayarla, aunque en su empeño deberá cubrir el valor de la tasa por Servicios Administrativos. Consta del

[522] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 008-17-SIS-CC], ROEC No. 7 (2 de mayo de 2017)
[523] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 046-17-SIS-CC], ROEC No. 77 (26 de abril de 2019)

> expediente que según certificación conferida el 4 de enero del 2008, por el Tesorero Municipal del Gobierno Municipal del Cantón Naranjal, la recurrente no adeuda valor alguno; por tanto, este aspecto no puede constituirse en un pretexto para desoír el anhelo de acceder a la información que sobre sus bienes tiene la recurrente a través del hábeas data, que como hemos señalado, es un recurso sencillo y ágil, cuyo objetivo es tutelar o garantizar derechos de las personas, tales como: el derecho a dirigir peticiones y a recibir atención a las mismas.[524]

Anotándose que dicha resolución establece además que no se puede dejar de atender la petición de acceso a información sobre sus bienes por no haberse pagado la tasa administrativa, tanto más que conforme consta en dicho texto el recurrente no adeudaba valor alguno. Todo ello porque, esta acción no puede estar limitada a condiciones formales que atenten contra su carácter ágil y sencillo de garantía inmediata de sus derechos.

La misma resolución precisa además que, es también parte del derecho constitucional, que la naturaleza de la información personal sea veraz, plural y oportuna, condiciones que son parte indiscutible del principio de calidad de datos.

> El derecho a acceder a fuentes de información, a acceder a documentos y bancos de datos; a buscar, recibir y conocer información objetiva, veraz, plural y oportuna sobre sí misma o sobre sus bienes, constituye un derecho constitucional. [525]

La finalidad del *habeas data* es obtener conocimiento de los datos del titular y de la finalidad de su recogida, aludiendo que estos pueden estar a cargo de responsables públicos o privados, tal como se señala el texto a continuación:

> [...] viene a estar considerada como un mecanismo de satisfacción urgente para que las personas puedan obtener el conocimiento de los datos a ellos referidos, y advertirse sobre su finalidad, sea que dicha información conste en el registro o banco de datos público o privado[526].

Otro de los derechos que otorga el *habeas data* es el reconocido en la resolución No. 032-15-SEP-CC que señala que ante la negativa del responsable de tratamiento sobre el derecho de acceso del titular está facultado a acudir al juez competente, al tenor de lo siguiente:

> La normativa y la jurisprudencia citadas son claras al determinar la naturaleza y objeto de la acción de hábeas data, mismas que radican en el derecho que tiene toda persona a acceder a los documentos de datos personales que sobre sí misma consten en entidades públicas o privadas, así como la posibilidad de acudir ante el juez competente cuando se le imposibilite el ejercicio de su derecho[527].

Adicionalmente, el *habeas data* tiene como objetivo proteger a las personas de usos inadecuados como los descritos a continuación:

> La acción de hábeas data sirve para proteger al ciudadano en caso de que el Estado o los particulares hagan uso de una información incorrecta, inexacta u obsoleta y que, al difundir tal información, se produzcan discrímenes, calificaciones deshonrosas, etc.[528]

---

[524] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 042-18-SIS-CC 42], ROEC No. 62 (19 de octubre de 2018)
[525] Ibíd., [Sentencia No. 042-18-SIS-CC 42]
[526] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 025-15-SEP-CC], ROS No. 485, (22 de Abril 2015).
[527] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 032-15-SEP-CC], ROS No. 462, (19 de Marzo de 2015).
[528] [Sentencia No. 019-09-SEP-CC2], en ROS, No.018 (3 de septiembre de 2009).

6.2.3.4 La transferencia de información sobre mora, sin condición de validez, vulnera el *habeas data* y el buen nombre

Respecto de información crediticia, se establece que no es suficiente la simple afirmación de que una persona está en mora sino que es indispensable demostrar su existencia como condición de validez, con la finalidad de evitar vulneraciones al *habeas data* y al buen nombre al tenor del siguiente análisis:

> Los bancos se encuentran en capacidad de reportar el comportamiento crediticio de sus clientes por lo que deben sustentar dicha información en obligaciones existentes y comprobables. Asimismo, en caso de que el reporte verse sobre el incumplimiento de dichas obligaciones, en miras de preservar el buen nombre de sus clientes, deben demostrar la existencia de la mora respectiva como condición de validez de los reportes que brinden a entidades como la central de riesgos. En caso de que estas condiciones no sean cumplidas y se proceda a la transferencia de información personal, se estará ante la vulneración del derecho a acceder al hábeas data del sujeto concernido, así como del derecho fundamental al buen nombre, lo que a su vez tiene incidencia en la conformación de barreras injustificadas para el acceso a los servicios comerciales y de crédito. Todos estos elementos que deben ser tomados en cuenta por los jueces constitucionales en conocimiento de acciones constitucionales como el hábeas data[529].

6.2.3.5 Acción de *habeas data* no puede usarse como vía de impugnación de un acto administrativo

Para evitar abusos procesales se determina que la acción de habeas data no podrá usarse para impugnar un acto administrativo, sino que deberá justificarse que a través de los datos personales se trasgrede el derecho a la autodeterminación informativa. En este sentido consta a continuación la cita de la sentencia:

> Puesto que, con absoluta claridad y de manera argumentada justifican que la acción de hábeas data propuesta por la legitimada activa, lejos de perseguir un fin acorde con su naturaleza, objeto y finalidad, está encaminada a cuestionar alegaciones sometidas a verificación y determinación previa; sin que se llegue a justificar la existencia del presupuesto contenido en el artículo 50 numeral 2 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. En este contexto, esta Corte resalta la argumentación del tribunal *ad quem*, en el sentido que la acción propuesta por la legitimada activa en representación de la "fundación "PIOCAMPE" no se encuentra en el supuesto de procedibilidad de tal acción, puesto que no busca que se rectifique información sobre la cual puede aseverarse su falta de veracidad; y por lo tanto afecte su derecho a la autodeterminación informativa. Contrario sensu, se advierte que la acción de hábeas data pretende buscar otra vía de impugnación de un acto administrativo, por cuanto, a criterio de la accionante, el mismo obedece a valoraciones erradas. Es decir, el asunto referente a la exactitud o veracidad de la información constante en el registro en

[529] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 008-16-SIS-CC], ROS No. 767 (2 de junio de 2016)

cuestión es un asunto debatido, por lo que mal se podría optar por una solicitud tendiente a su rectificación[530].

6.2.3.6 Procede *habeas data* en contra Ministerio por mantener un impedimento y abstenerse de actualizar de datos personales por solicitar requisitos adicionales

La demora en un reingreso laboral causada por una entidad pública que no atiende de forma oportuna una actualización de datos personales, solicitada por su titular, determina la existencia de un daño y por lo tanto la procedencia del *habeas data*, de conformidad con la resolución que en su parte pertinente se cita a continuación:

> Por tanto, de conformidad con el precepto constitucional citado, y en correspondencia con el argumento utilizado por la Segunda Sala de Garantías Penales de la Corte Provincial de Justicia de Pichincha, el Ministerio de Relaciones Laborales, por el transcurso del tiempo previsto en la ley, debía retirar el impedimento legal que constaba en la base de datos para que el señor Néstor Manuel Tapia Bolaños pueda efectuar su reingreso laboral sí así lo quería. Entonces, el Ministerio de Relaciones Laborales, al mantener un impedimento y abstenerse de efectuar la actualización de datos personales del señor Néstor Manuel Tapia Bolaños, con el pretexto de requerir más requisitos para la actualización de la información que el transcurso del tiempo, incurrió a juicio de la Sala en un acto que determinó la procedencia de la acción constitucional incoada[531].

6.2.3.7 No procede accionar *habeas data* para anular un acto administrativo que reconoce el derecho a efectuar un acto civil

Es improcedente utilizar la acción de *habeas data* para eliminar la actuación de una autoridad pública, en este caso, la razón de un Registrador de la Propiedad, pues la vía pertinente para su revisión es la jurisdiccional, tal como consta en la cita que consta a continuación:

> [...] la pretensión de la accionante se dirige a eliminar una razón puesta por el Registrador de la Propiedad al margen de una escritura, por lo cual en un acto administrativo, cuya legitimidad no puede ser analizada en acción de Hábeas Data, anula un acto civil. Es decir, no pretende la anulación de información que pudiera causar daño a su intimidad, privacidad, identidad, confidencialidad o autodeterminación informativa, sino que, por vía constitucional pretende la anulación de un acto administrativo que implica el reconocimiento del derecho a efectuar un acto civil. Si bien la información a la que se refiere el Hábeas Data, puede ser personal o relacionada con los bienes de una persona, en el presente caso, la pretensión del accionante no evidencia un afán de protección de información, sino que pretende eliminar una actuación de autoridad pública, que presume ilegítima y cuya declaratoria en este sentido corresponde a las autoridades jurisdiccionales competentes, pero no puede pretenderse por vía de Hábeas Data [...][532]

[530] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 386-16-SEP-CC], ROEE No. 852 (24 de enero de 2017)
[531] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 312-17-SEP-CC], ROEC No. 22 (05 de diciembre de 2017)
[532] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 131-17-SEP-CC], ROEC No. 6 (3 de julio de 2017)

6.2.3.8 Constitucionalidad de la Regulación No. 029-2012 que ordena el reporte diario al Banco Central del Ecuador de las transferencias de dinero provenientes del exterior

En cumplimiento de la atribución contenida en el artículo 436, número 2, de la Constitución, en concordancia con el artículo 90 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional se solicita la inconstitucionalidad por el fondo y por la forma de la Regulación No, 029-2012, emitida por el Directorio del Banco Central del Ecuador, el 11 de julio de 2012, Registro Oficial No. 755 de 27 de julio de 2012. Respecto de esta petición, la resolución que se cita a continuación señala que:

> […] es menester referirnos al contenido de las normas constitucionales, que el accionante considera son violentadas con la presente resolución que son los artículos 66 numeral 19; 92 y 231 de la Constitución de la República del Ecuador [que] se refieren respectivamente al derecho a la protección de datos de carácter personal; la acción de hábeas data; y, la obligación de las servidoras y servidores públicos de efectuar una declaración patrimonial jurada de activos y pasivos, al iniciar y finalizar su gestión, lo cual debe ser corroborado por la Contraloría General del Estado. En aquel sentido, la Corte no advierte en qué medida el hecho de que las entidades del Sistema Financiero Nacional reporten diariamente al Banco Central del Ecuador, las transferencias de dinero provenientes del exterior efectuadas el día laborable inmediato anterior, entra en contradicción o comporta una vulneración de las normas antes desarrolladas; máxime cuando tal entrega de información, obedece a la formulación de políticas monetaria, crediticia, cambiaría y financiera, en relación con la obligación que ostenta el Estado, a través de todos los organismos de control -Contraloría General del Estado, superintendencias y otros- de ejercer el control de estas políticas, para garantizar adecuados márgenes de seguridad financiera y orientar los excedentes de liquidez hacia inversión requerida para el desarrollo del país. Además, no debe perderse de vista que el Banco Central del Ecuador como receptor de la información, también se encuentra sujeto a la Norma Suprema y en aquel sentido, tiene el deber de la protección de la información que le sea entregada; a menos que existan excepcionalidades por asuntos de investigación o judiciales, que deba otorgar dicha información a otras entidades. En virtud de aquello, la Corte Constitucional del Ecuador concluye que los artículos 2 y 7 de la Resolución No. 52-2015-F de la Junta de Política Monetaria y Financiera, publicada en Registro Oficial No. 489 del 28 de abril de 2015, no contravienen lo previsto en los artículos 66 numeral 19; 92 y 231 de la Constitución de la República del Ecuador[533].

De la cita que antecede podemos colegir que la entrega de información personal para favorecer la formulación de políticas monetaria, crediticia, cambiaría y financiera, y de su respectivo control no entra en contradicción o vulnera el derecho a la protección de datos personales, el *habeas data* o la obligación de efectuar declaraciones patrimoniales.

6.2.3.9 Es parte fundamental del *habeas data* la autodeterminación informativa que permite la tutela del derecho a la protección de datos personales

Si bien la jurisprudencia obligatoria ya ha señalado que la autodeterminación informativa es parte del derecho a la protección de datos personales.[534] La sentencia que se cita a

[533] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 026-17-SIN-CC], ROEC No. 22 (5 de diciembre de 2017)
[534] Ibíd., [Sentencia No. 001-14-PJO-CC], en ROS, No. 281 (2 de julio de 2014).

continuación sostiene que la autodeterminación informativa es parte fundamental del *habeas data* y permite la tutela de varios derechos entre ellos el relativo a la protección de datos personales:

> […] la acción de hábeas data tiene como elemento esencial el control de los datos que existan sobre una persona o sobre sus bienes -o lo que jurídicamente se conoce como autodeterminación informativa- a fin de tutelar derechos constitucionales como el derecho a la intimidad personal y familiar, a la honra, a la buena reputación y a la protección de datos de carácter personal; es por ello que, el objetivo de esta garantía jurisdiccional se dirige específicamente a buscar la rectificación, actualización o eliminación de datos personales, cuando esta información pueda causar algún tipo de perjuicio para la persona o pueda transgredir los derechos constitucionales antes referidos.[535]

6.2.3.10 La acción de *habeas data* en la actual Constitución mantiene similar configuración a la contenida en la anterior Norma Constitucional

Debido a demoras procesales, varios recursos de *habeas data* propuestos al amparo de la Constitución de 1998 han llegado a conocimiento de la actual Corte Constitucional. En virtud de la disposición transitoria primera prevista en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional estas causas deberán sustanciarse de conformidad con la normativa adjetiva vigente al momento de iniciar su trámite, y además armonizarse con la Constitución de la República vigente.

De tal forma que, respecto de la acción de *habeas data* se ha dictado el criterio que se analiza a continuación:

> En este contexto se considera oportuno señalar, que la acción de hábeas data en la actual Constitución mantuvo similar configuración a la contenida en la anterior Norma Constitucional; razón por la cual, el análisis a realizarse al amparo de uno u otro cuerpo normativo, es en esencia el mismo, pues no se verifican diferencias de carácter sustancial que impliquen un cambio en la noción de esta garantía jurisdiccional.[536]

En el mismo sentido, la sentencia que consta a continuación señala que:

> […] la conceptualización de la acción de hábeas Data en el actual orden constitucional, no muestra diferencia de carácter sustancial respecto a la Constitución Política de 1998; pues, el constituyente mantuvo el núcleo esencial de esta garantía jurisdiccional, que es dotar a las personas de un medio constitucional para conocer la información personal que reposa en entidades públicas y privadas, evitar que esta sea utilizada en forma indebida y permitir su rectificación o eliminación, en el caso que aquella atente contra sus derechos constitucionales.[537]

Si bien, el interés fundamental del *habeas data* es el mismo, sin embargo, se ha ampliado su ámbito de aplicación, pues ahora incluye el soporte electrónico, y se han eliminado formalidades para su presentación y sustanciación, tal como se señala a continuación:

> De lo señalado, se colige que el objeto y ámbito de protección de esta garantía jurisdiccional es esencialmente el mismo, en tanto, la configuración del hábeas data dentro de las Constituciones de 1998 y 2008, reflejan un interés primordial por tutelar el derecho a la protección de datos de carácter personal, el derecho a la intimidad personal, así como otros derechos conexos y relativos al acceso y protección de la información personal de cada

[535] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0001-16-HD], ROEC No. 1 (20 de marzo de 2017) Ibíd., [Sentencia No. 025-15-SEP-CC], ROS No. 485, (22 de Abril 2015).
[536] Ibíd., [Sentencia No. 0002-14-HD] en ROEC, No. 2 (5 de junio de 2017)
[537] Ibíd., [Sentencia No. 0001-15-11D], en ROEC, No. 70 (29 de marzo de 2019).

> individuo. Sin embargo, no se puede dejar de reconocer que sí han existido cambios respecto al hábeas data en la actual Norma Suprema, estos se han orientado a procurar un ámbito de protección más amplio y eficaz de los derechos constitucionales tutelados por esta garantía, así por ejemplo según señala el artículo 92 de la Constitución de la República vigente, el hábeas data permite también el acceso a datos e información que se encuentra en soporte electrónico; además de ello, como todas las garantías jurisdiccionales en general, la acción de hábeas data se encuentra desprovista de excesivas formalidades para su presentación y sustanciación.[538]

6.2.3.11 No se requiere de abogado para interponer acción de *habeas data*

Con la finalidad de acercar esta garantía a la ciudadanía, ya no se necesita del patrocinio de un abogado para la interposición de una acción de *habeas data*. Sin duda esta intención es positiva, sin embargo por la naturaleza técnica y el desarrollo de las TIC se hace difícil comprender las repercusiones del uso inadecuado de los datos personales.

Por ello, no es suficiente una legitimación abierta sino además el desarrollo simultáneo de una cultura de protección que permita a los titulares un acceso real a esta garantía. A continuación la cita de la resolución:

> Es preciso señalar que el hábeas data en Ecuador, actualmente refleja madurez jurídica en la medida que sus avances normativos en el plano procesal se han desarrollado para acercar la garantía a la ciudadanía. Esto con el hecho de que la legitimación amplia hace que ya no se necesita el patrocinio de un abogado para la presentación de la solicitud o la demanda, y se ha buscado una verdadera desconcentración judicial al encontrar que en una segunda instancia ya no es el máximo órgano de administración de justicia constitucional el encargado de conocer la impugnación, sino que será la corte provincial la que conozca y resuelva el proceso en alzada.[539]

[538] Ibíd., [Sentencia No. 0001-16-HD], ROEC No. 1 (20 de marzo de 2017)
[539] Ibíd.

7. Innovación ecuatoriana: la reparación integral en la protección de datos personales y la nueva configuración del *habeas data* restaurador. El *habeas data* no limitado a la simple indemnización

Dentro del sistema de protección de derechos instaurado en la vigente Constitución, uno de los elementos fundamentales es la incorporación de la reparación integral. El artículo 86 de la CRE que da inicio al Capítulo Tercero, que se refiere a las Garantías Constitucionales, señala las disposiciones generales que regulan de forma obligatoria a las diferentes garantías jurisdiccionales existentes, entre las cuales consta el *habeas data*. El numeral tercero del citado artículo 86, expresamente, incluye como obligación de los jueces, al momento de dictar sus sentencias, ordenar la reparación integral material e inmaterial del derecho lesionado; además de especificar e individualizar las obligaciones, positivas y negativas, del destinatario de la decisión judicial y las circunstancias en que dichas obligaciones deban cumplirse.

Por tratarse de derechos fundamentales, las garantías constitucionales que los protegen no pueden tener como única consecuencia la reparación económica. Motivo por el cual, la reparación integral es la pertinente, ya que permite no solo reparar los daños materiales (daño emergente, lucro cesante, proyecto de vida, costas y gastos), sino también los daños inmateriales[540] e incluso dictarse otras formas de reparación propias del sistema de defensa de derechos humanos como son las medidas de satisfacción (que buscan reparar el daño inmaterial, que no tienen alcance pecuniario) y las garantías de no repetición[541] (medidas de alcance o repercusión pública), conforme ha señalado en varias resoluciones la Corte Interamericana de Derechos Humanos: Blanco Romero y otros; García Asto y Ramírez Rojas; y Gómez Palomino[542].

Es indispensable incluir y aplicar el principio de la *restituto in integris* que se diferencia de la indemnización, porque se configura como resarcimiento inmaterial, y además determina que el proceso ya no termina con la sentencia, sino solo cuando se haya conseguido la reparación integral del daño.[543] Por tal motivo, se ha señalado que la propia sentencia es un mecanismo

[540] "El daño inmaterial puede comprender tanto los sufrimientos y las aflicciones causados a las víctimas directas y a sus allegados, como el menoscabo de valores muy significativos para las personas, así como las alteraciones, de carácter no pecuniario, en las condiciones de existencia de la víctima o su familia. No siendo posible asignar al daño inmaterial un preciso equivalente monetario, sólo puede, para los fines de la reparación integral a las víctimas, ser objeto de compensación, y ello de dos maneras. En primer lugar, mediante el pago de una cantidad de dinero o la entrega de bienes o servicios apreciables en dinero, que el Tribunal determine en aplicación razonable del arbitrio judicial y en términos de equidad. Y en segundo lugar, mediante la realización de actos u obras de alcance o repercusión públicos, tales como la transmisión de un mensaje de reprobación oficial a las violaciones de los derechos humanos de que se trata y de compromiso con los esfuerzos tendientes a que no vuelvan a ocurrir, que tengan como efecto la recuperación de la memoria de las víctimas, el reconocimiento de su dignidad y el consuelo de sus deudos". CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso Gómez Palomino vs. Perú], p. supra nota 11, ¶ 130.

[541] *Programa de educación. Reformas normativas* locales. CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso Gómez Palomino vs. Perú].

[542] Obligación de investigar los hechos denunciados, identificar, juzgar y sancionar a los responsables. Obligación de buscar los restos mortales de la víctima y entregarlos a sus familiares. Publicación de Sentencia de la Corte. Asistencia médica y psicológica. CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso Gómez Palomino vs. Perú], cit. *Reconocimiento simbólico [por parte del Estado] destinado a la recuperación de la memoria histórica de las personas desaparecidas.* CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso Blanco Romero y Otros vs. Venezuela]. Ser objeto de una satisfacción de carácter moral públicamente y con trascendencia. (Disculpas públicas) CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso García Asto y Ramírez Rojas].

[543] C. STORINI, "Las garantías constitucionales", 307.

de reparación;[544] además la materialización de la reparación integral es uno de los mecanismos fundamentales para garantizar la efectividad de las decisiones judiciales.[545] En la sentencia No. 001-10-PJO-CC consta expresamente que:

> [...] el mecanismo de cumplimiento de sentencias propende a la materialización de la reparación integral adoptada dentro de una garantía jurisdiccional. La Corte Constitucional, de oficio o a petición de parte, considerando que de por medio se encuentra la materialización de la reparación integral, y sin necesidad de que comparezca exclusivamente el afectado, está en la obligación de velar por el cumplimiento de las sentencias constitucionales.[546]

Consecuente con la figura de reparación integral desarrollada ampliamente por el sistema interamericano de derechos humanos, el artículo 18 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional recoge una lista variada de mecanismos distintos a la simple indemnización que pretenden, en la medida de lo posible, devolver el daño al estado anterior, como si este nunca se hubiese producido. En tal caso, de ser procedente la declaración de vulneración de derechos se ordenará la reparación integral por el daño material e inmaterial. Pero además, conforme el mencionado artículo, la reparación integral:

> [...] procurará que la persona o personas titulares del derecho violado gocen y disfruten el derecho de la manera más adecuada posible y que se restablezca a la situación anterior a la violación. La reparación podrá incluir, entre otras formas, la restitución del derecho, la compensación económica o patrimonial, la rehabilitación, la satisfacción, las garantías de que el hecho no se repita, la obligación de remitir a la autoridad competente para investigar y sancionar, las medidas de reconocimiento, las disculpas públicas, la prestación de servicios públicos, la atención de salud.

Además del régimen de aplicación general para las garantías constitucionales constante en el artículo 86 CRE que establece la reparación integral, la parte final del artículo 94 de la CRE, que desarrolla la acción de *habeas data*, faculta a la persona afectada a demandar por los perjuicios ocasionados.

Estos perjuicios podrán ser reparados integralmente, no solo en aplicación directa del texto constitucional invocado, sino en cumplimiento de lo dispuesto por la Ley Orgánica de

---

[544] CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso Raxcacó Reyes vs. Guatemala], p. supra nota 4, ¶ 131. En el mismo sentido las siguientes resoluciones: CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso Acosta Calderón vs. Ecuador], p. supra nota 3, ¶ 159; [Caso Yatama vs. Nicaragua], p. supra nota 3, ¶ 260; [Caso "Masacre de Mapiripán" vs. Colombia], p. supra nota 1, ¶ 285; [Caso Gutiérrez Soler vs. Colombia], p. supra nota 4, ¶ 83.

[545] El numeral 4 del artículo 86 de la CRE establece sistemas de responsabilidad tanto para personas públicas como privadas en el caso de incumplimiento de una sentencia en materia de garantías jurisdiccionales. El artículo 436 numeral 9 otorga competencia a la Corte Constitucional para conocer y sancionar este incumplimiento. Ante la necesidad de una justicia efectiva, no es suficiente con dictar una sentencia que favorezca a una de las partes, sino que es menester que esta se cumpla por parte de los obligados; y que, aun contra su voluntad, las autoridades constitucionales la hagan cumplir. La sentencia No. 001-10-PJO-CC considera que "los mecanismos de cumplimiento de sentencias, resoluciones y dictámenes constitucionales se constituyen per se en auténticas garantías jurisdiccionales de protección y reparación de derechos constitucionales, si no existieran mecanismos de cumplimiento como los señalados, de nada serviría la presencia de garantías para la protección de todos los derechos constitucionales". Esta afirmación jurisprudencial, se sustenta a su vez en otras sentencias provenientes del sistema internacional humanitario, dictadas por la Corte Interamericana en los casos Baena Ricardo y otros, y Acevedo Jaramillo que señala: "La efectividad de las sentencias depende de su ejecución. El proceso debe tender a la materialización de la protección del derecho reconocido en el pronunciamiento judicial mediante la aplicación idónea de dicho pronunciamiento".

[546] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0023-2008-HD].

Garantías Jurisdiccionales y Control Constitucional en el artículo 49 que aclara, respecto de las sentencias de garantías jurisdiccionales, en este caso del *habeas data*, que "El concepto de reparación integral incluirá todas las obligaciones materiales e inmateriales que el juez determine para hacer efectiva dicha reparación".

En consecuencia, la normativa ecuatoriana supera el contenido tradicional de *habeas data* y establece no solo su carácter informativo, aditivo, rectificador y correctivo, exclutorio, reservado, cancelatorio, indemnizatorio etc., sino especialmente su finalidad reparadora. Es decir, la norma ecuatoriana no se limita al tradicional sistema de responsabilidad por daño causado que permite el derecho a recibir una indemnización, sino que utiliza una institución propia de los derechos humanos: la reparación integral.

Conforme se ha analizado previamente, el *habeas data* en la Constitución vigente se configura como una garantía jurisdiccional que no se limita a regularizar documentos, datos genéticos, bancos o archivos de datos personales e informes sobre sí mismos o sobre sus bienes, o sea, al acceso, eliminación, actualización, rectificación o anulación. Sino que, entre sus finalidades también se incluye la de verificar que estos datos personales no hayan sido utilizados como mecanismos de discriminación, mediante valoraciones equivocadas de datos o por "agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos". En este sentido, el artículo 50 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional señala que "Se podrá interponer la acción de hábeas data en los siguientes casos: [...] c) Cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente".

De ese modo, la voluntad del legislador al incluir en la norma relativa al *habeas data* un acápite sobre la reparación integral tiene como intencionalidad que, mediante la reparación integral se logren evitar potenciales, existentes o futuros daños no solo con la supresión, eliminación, cancelación del dato, sino corregir actos discriminatorios y establecer otras obligaciones materiales e inmateriales para hacer efectiva la reparación.

En otras palabras, el carácter reparador del *habeas data* garantiza el verdadero contenido del derecho a la protección de datos, relativo no solo a la autodeterminación informativa, sino sobre todo a la eliminación a título de reparación integral, de todas aquellas consecuencias dañosas y discriminatorias que hayan provenido de la utilización de datos, no solo de aquellos sensibles sino incluso de los inocuos que, sin embargo, causan transgresiones a la dignidad y a la libertad de las personas.

El reconocimiento constitucional del derecho a la protección de datos y del *habeas data*, así como el desarrollo del *habeas data* en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, establecen que en Ecuador existe un progreso normativo en el derecho y su garantía constitucional, que incluso supera a otras legislaciones, al reconocer un nivel aun mayor de protección mediante el *habeas data* reparador o reparatorio; no obstante, aún prevalecen en nuestros tribunales criterios extraídos del anterior sistema de protección de los datos personales asociados a la intimidad.

Dicho de otra manera, aún no se ha configurado a nivel jurisprudencial una aplicación de la verdadera naturaleza del derecho a la protección de datos de carácter personal como garantía de otros derechos, puesto que aunque se reconoce en varias resoluciones del año 2008 que el *habeas data* es "una garantía constitucional que tiene por objeto proteger el acceso a la

información personal, así como el derecho a la honra, a la buena reputación y a la intimidad personal y familiar; en consecuencia es derecho de toda persona para acceder a los documentos, banco de datos o informes que sobre sí misma, o sus bienes consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellas y su propósito".[547] Sin embargo, las sentencias en su parte resolutiva aún no incluyen la satisfacción de otros derechos fundamentales distintos a la intimidad o a otros derechos fundamentales incluido el derecho a la protección de datos personales.

Para ejemplificar lo señalado, la Corte Constitucional ecuatoriana en Sentencia No. 0019-09-SEP-CC de 2009-08-06, Caso 0014-09-EP, Publicado en el RO, No. 018 (03 de septiembre de 2003) dice:

> [...] El *habeas data* es una garantía que protege varios derechos, tales como: la información, la honra, la buena reputación y la intimidad. Al ser el *habeas data*, una garantía jurisdiccional cautelar, no procede **por esta vía la declaración o reconocimiento de derechos,** mucho menos de aquellos que son inexistentes [...]. En conclusión, en **estricto cumplimiento a la naturaleza del *habeas data*, no procede, mediante esta vía, declarar la condición de jubilado** y mucho menos disponer la restitución de una condición inexistente... (énfasis añadido).

Como se lee en el texto citado, no se admite a efecto de reparación integral el que pueda declararse la vulneración de un derecho, como en este caso el de jubilación, y en consecuencia dictaminar en la sentencia no solo la rectificación del dato en un fichero, sino su efectiva vigencia y reconocimiento no solo de carácter económico, sino de restablecimiento del derecho vulnerado, tal como señala la naturaleza de la reparación integral.

8. La protección de datos personales y otros derechos fundamentales: principio de proporcionalidad y ponderación

La protección de datos personales construye su contenido esencial, principalmente, mediante las limitaciones legales existentes, y además de las características diferenciadoras producto de la fricción con otros derechos hermanos, hijos de la privacidad, como son: la inviolabilidad del domicilio y de la correspondencia, el honor, la intimidad, la imagen y la propia voz.

Ahora bien, la esencialidad de un derecho también se pone de manifiesto cuando entra en conflicto e incluso en contradicción con otros derechos que pertenecen a diferentes ámbitos de protección del ser humano.

En la jurisprudencia extranjera, varios de los casos de conflicto de derechos se relacionan con el derecho a la libertad de expresión, libertad de información, cobro de impuestos, deudas con en el sistema financiero, servicios administrativos y seguridad ciudadana, entre ellos podemos destacar el caso *Lindqvist*[548] con sentencia emitida el 06 de noviembre de 2003 y resuelta por el Tribunal de Justicia de la Unión Europea, así también el caso *Satakunnan*

[547] Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR PARA EL PERIODO DE TRANSICIÓN, [Sentencia No. 0074-2008-HD], en ROS, No. 8 (4 de septiembre de 2009); [Sentencia No. 0039-2008-HD], en ROS, No. 86 (05 de diciembre de 2008); Sentencia No. 0076-2008-HD], en ROS, No. 111 (25 de marzo de 2009); Sentencia No. 0051-2008-HD, en ROS, No. 531 (18 de febrero de 2009); Sentencia No. 0079-2008-HD], en ROS, No. 8 (4 de septiembre de 2009); Sentencia No. 0003-2009-HD, en ROS, No. 122 (13 de mayo de 2009).
[548] Lindqvist (C-101), *Petición de decisión prejudicial*, de 6 de noviembre de 2003

Markkinapörssi[549] con sentencia emitida el 16 de diciembre de 2008 por el mismo tribunal. Asimismo, gran parte de ellos, tal y como logramos observar en los casos previamente propuestos, se han resuelto desde la voluntariedad del titular del dato y, en ausencia de esta, de los mandatos o autorizaciones legales, motivadas en intereses generales que favorecen a la sociedad.

Sin embargo, existen otros casos en los que no existe disposición legal que permita dilucidar con claridad qué derecho prima, debido a que la transgresión se manifiesta en la práctica de derecho y la solución no pudo ser prevista por el legislador. En estos casos, las sentencias judiciales dictadas por Cortes Constitucionales aplicando el principio de proporcionalidad y la interpretación constitucional debieran resolver qué derecho prima, y en consecuencia garantizar a la persona un grado máximo de protección de sus derechos.

De la investigación realizada a las sentencias dictadas desde el año 2008 hasta el 2019, se puede colegir que no se ha puesto en conocimiento de la Corte Constitucional del Ecuador ningún caso de conflictos de derechos en los cuales sea pertinente aplicar el principio de ponderación.

A nivel constitucional los derechos tienden a formularse predominantemente como principios; es decir, como directrices genéricas y abstractas, lo cual provee un apreciable margen de interpretación que hace posible el ulterior desarrollo legislativo y político de estos mismos derechos. Es en la legislación y en las políticas públicas que estos derechos se concretan en reglas, o sea, en normas específicas que detallan titulares, conductas y sanciones, que excluyen aquellas regulaciones claramente contrarias a los fines y valores que los derechos a nivel constitucional han establecido.[550]

Esa situación no significa que no exista un conflicto de derechos. Para ello se citará, a manera de ejemplo, un estudio realizado sobre la base judicial accesible al público de forma *on line* denominado Sistema Automático de Trámite Judicial Ecuatoriano (SATJE).[551]

El sistema judicial ecuatoriano señala como uno de sus pilares fundamentales al principio de publicidad. El artículo 165 numeral 5 de la CRE, respecto de los principios que la administración pública debe cumplir, señala: "5. En todas sus etapas, los juicios y sus decisiones serán públicas, salvo los casos expresamente señalados en la ley". La importancia de este principio radica en que "permite establecer si los jueces son probos, independientes e imparciales, si respetan el debido proceso en las causas a su cargo y si ayudan a consolidar la seguridad jurídica".[552]

Sin embargo, este principio como cualquier otro tiene excepciones marcadas por la ley; por ejemplo, el Código Orgánico Integral Penal[553] respecto a la privacidad y confidencialidad de

[549] SATAKUNNAN MARKKINAPÖRSSI, [Petición de decisión prejudicial (C-73/07)], de 16 de diciembre de 2008
[550] A. GRIJALVA, *Constitucionalismo en Ecuador*, 64.
[551] REYES AMÁN, JONNATHAN, "Derecho a la protección de datos personales en las bases de datos judiciales accesibles al público en temas de niñez y adolescencia" (trabajo de titulación para la obtención del grado profesional de abogado del Ecuador, Universidad de las Américas, 2016).
[552] M. J. RODRÍGUEZ VILLAFAÑEZ, "La transparencia en el Poder Judicial de Argentina, Reforma Judicial", *Reforma Judicial, Revista Mexicana de Justicia*, vol. 2 (2003): 169. ‹ http://revistas.juridicas.unam.mx/index.php/reforma-judicial/article/view/8567/10590›. Consulta: 23 de agosto de 2016.
[553] Ecuador, ASAMBLEA NACIONAL DEL ECUADOR, *Código Orgánico Integral Penal*, en ROS, No. 180 (10 de febrero de 2014). ‹http://www.asambleanacional.gob.ec/es/leyes-aprobadas›. Consulta: 18 de febrero de 2018.

los procesos judiciales en los que estén involucrados niños, niñas y adolescentes. Incluso de forma general el artículo 8 del Código Orgánico General de Procesos,[554] sobre el principio de publicidad señala excepciones estrictamente necesarias para proteger la intimidad, el honor, el buen nombre o la seguridad de cualquier persona. En tal sentido, serán reservadas las diligencias y actuaciones procesales previstas como tales en la Constitución de la República y la ley (Código Orgánico General de Procesos, 2015, artículo 8).[555]

La práctica generalizada, no obstante, es que el sistema de consultas judiciales SATJE permite el acceso a todo tipo de información procesal que consta descrita en las actuaciones judiciales digitando los nombres de las personas. En el estudio citado se recogen ejemplos emblemáticos de esta transgresión ya que este portal, al no estar diseñado acogiendo los principios de la protección de datos personales, permite tener acceso a datos de niños, niñas y adolescentes, incluso en aquellos casos que están prohibidos legalmente.

Ahora bien, este sistema de acceso *on line*, SATJE, sustenta su estructura de servicio en el principio de publicidad; en otras palabras, está diseñado para, mediante el nombre de actores o demandados, visibilizar cada una de las actuaciones judiciales, incluida la sentencia. En todos estos actos procesales consta, de forma íntegra, los nombres de las partes intervinientes. Se puede, entonces, por medio de la simple lectura del proceso encontrar y asociar datos personales facilitados por las partes para impulsar un proceso, para sustentar sus afirmaciones, alegaciones o pretensiones incluyendo datos sensibles.

Es ahí cuando aparece el conflicto de derechos, pues frente a esta aplicación o compresión del principio de publicidad de los procesos judiciales entra en conflicto el derecho a la protección de datos personales; por tanto, se pueden encontrar mecanismos, protocolos o principios que permitan regular la forma de acceso a los actos procesales y al mismo tiempo no develar datos personales de los partícipes de un litigio judicial. Dicho de otro modo, limitar la publicidad judicial a favor del derecho a la protección de datos personales. Quienes están a favor de esta postura sostienen que la omisión de los nombres o la anonimización de las actuaciones judiciales que se publicitan por distintos medios, o la limitación del acceso a las actuaciones judiciales en los que consten el nombre de las partes solo a personas que tengan interés legítimo en el proceso, no afecta el principio de publicidad, ya que en esencia lo que interesa es que se emitan resoluciones judiciales debidamente motivadas como garantía de imparcialidad, independencia, probidad y democracia.

Rosario Duaso Calés, respecto a los documentos públicos que son accesibles por internet y la protección de datos personales sostiene: "podemos afirmar que, un dato de carácter personal, aunque se haya hecho público, debe seguir siendo protegido, ya que no pierde su carácter de dato personal. Pero, el problema principal para que esta protección se haga efectiva reside en el hecho de que una vez que se han hecho públicos o accesibles a la ciudadanía estos datos, la divulgación imposibilita de forma radical la protección que les debe ser acordada...".[556]

---

[554] Ecuador, ASAMBLEA NACIONAL DEL ECUADOR, *Código Orgánico General de Procesos*, en ROS, No. 506 (22 de mayo de 2015).
[555] Ibíd.
[556] R. DUASO CALÉS, "Regulación Europea sobre difusión de la jurisprudencia en internet
", en *Buenas Prácticas para la implementación de soluciones tecnológicas en la administración de justicia* (México: IIJusticia, Instituto de Investigación para la Justicia, 2011), 2. ‹http://www.iijusticia.org/heredia/PDF/Duaso.pdf›.

Dicho de otra manera, hay suficientes argumentos para que exista un conflicto real de derechos por las posibles transgresiones e implicaciones de los datos de las personas en expedientes judiciales físicos o virtuales. En consecuencia, el debate sobre el derecho que debe garantizarse puede elevarse a la Corte Constitucional, la cual deberá dilucidar mediante la ponderación de estos derechos, cuál de ellos presenta mayor posibilidad de daño, de producirse una transgresión, y por lo tanto privilegiarse su protección.

Ahora bien, en un análisis preliminar sobre los requisitos que necesariamente han de exigirse a cualquier limitación externa y legítima a los derechos constitucionales,[557] se podría señalar:

a) **Identificación de dos derechos o bienes constitucionales protegidos:** En el ejemplo planteado entran en conflicto el principio de publicidad judicial y el derecho a la protección de datos personales.

b) **No afectación del contenido esencial:** El contenido esencial del principio de publicidad no se vería afectado por anonimización de las sentencias judiciales, porque su importancia radica en la visibilización y transparencia de la actuación judicial mediante la motivación de sus decisiones, el debido proceso y la seguridad jurídica en el uso del precedente jurisprudencial obligatorio. Asimismo, el contenido esencial del derecho a la protección de datos personales sí se vulnera, pues los datos personales solo pueden ser recopilados y difundidos cuando existe una autorización judicial que se justifique en un interés social preponderante. En este caso, conocer el nombre de quien interviene en un acto procesal o ha sido favorecido o perjudicado por una sentencia puede serle útil a su titular o los directamente afectados, pero no necesariamente a todos los usuarios de internet. Esta situación de vulnerabilidad del ciudadano se pone en evidencia aún más cuando los nombres de las personas se asocian a datos incluso de carácter sensible que constan expresamente detallados en las actuaciones judiciales. Los datos personales deben ser protegidos en su conjunto, no solo de aquellos datos considerados íntimos, sino de todos aquellos que permitan una identificación completa del individuo, pues conllevan a realizar juicios de valor no necesariamente cercanos a la realidad y que puedan generar actos de discriminación y afectar el derecho a la autodeterminación informativa, el libre desarrollo de la personalidad y otros derechos específicos.

c) **Adecuación de la medida restrictiva al fin perseguido:** Es decir que la medida adoptada se conforme como un instrumento adecuado para conseguir el fin legítimo pretendido.[558] En este caso, la utilización de sistemas de anonimización y acceso al nombre de las partes procesales solo a quienes presenten un interés legítimo, así como acceso total al contenido de las actuaciones judiciales omitiendo los nombres no afecta el principio de publicidad de las actuaciones judiciales, como se vio anteriormente, pues su finalidad es precautelar la probidad de la actuación judicial.

d) **Indispensabilidad de la medida restrictiva:** Esto es que la restricción no tiene otra alternativa o medida menos agresiva para obtener la finalidad que se pretende.[559] Mantener el actual sistema de apertura ilimitada de datos personales en el sistema SATJE vulnera la protección de datos personales y no favorece el principio de publicidad. Al contrario, pone en peligro a los ciudadanos quienes, por ejemplo,

[557] M. APARICIO PÉREZ Y M. BARCELÓ I SERRAMALERA, edit., *Curso de derecho constitucional*, 614.
[558] Ibíd., 613.
[559] Ibíd.

intentan acceder a un empleo, un préstamo, una beca, entre otros y sus postulaciones son negadas porque empleadores, bancos o entidades de educación pueden acceder libremente a datos personales que no debieran estar disponibles de forma desproporcionada. No existen estudios sobre la plataforma que determinen el volumen o casos de usos distintos al de garantía del debido proceso y probidad judicial, que son las finalidades propias de la publicidad judicial, pero es práctica generalizada su utilización en las áreas de recursos humanos de las empresas, por ejemplo.

e) **Proporcionalidad en sentido estricto:** Se debe buscar un equilibrio razonable entre la porción desechada del derecho y el bien que, en cambio, se consigue.[560] La porción del derecho que no se aplicaría es minúscula, tanto que para el ejercicio del derecho de vigilancia de las actuaciones judiciales, mediante la difusión de actuaciones judiciales y del ejercicio del derecho a la defensa, puesto que en el primer caso, la sentencia no necesita de los nombres de las partes procesales y, en el segundo, este derecho se ejerce desde la notificación en debida forma de las actuaciones judiciales no de su publicación en el sistema SATJE. Ni aun en los casos de delitos penales, tanto más que actualmente existe en Ecuador una disposición constitucional que impide la discriminación por pasado judicial (ver artículo 11, numeral 2 de la CRE).

En conclusión, será la Corte Constitucional la que en cada caso particular puesto a su conocimiento aplique el método de interpretación de los mandatos de optimización, mediante la ponderación en sentido lato, conformado por los test de adecuación, test de necesidad y el test de proporcionalidad; y de la ponderación en sentido estricto, compuesto por la ley de ponderación, la fórmula del peso y las cargas de argumentación para establecer en cada caso concreto, por medio de un sentencia, cuál es el derecho que se privilegia.

9. Crítica a la normativa constitucional ecuatoriana respecto de su forma de reconocer el derecho a la protección de datos personales

Los incesantes avances tecnológicos, que se potencian día tras día, ya no solo se manifiestan en la recolección y manipulación de datos mediante canales como el teléfono, la navegación por internet y las bases de datos, sino de la utilización de nuevos elementos como: brazaletes de salud, que transmiten datos médicos en tiempo real, drones con videograbación y la geolocalización como elemento estructural para el funcionamiento de cada uno de los dispositivos y *softwares* existentes en el mercado.

Esos avances tecnológicos y otros que se manifiestan constantemente ponen en riesgo varios derechos de las personas. Se vuelve fundamental que el derecho responda a las necesidades actuales con rapidez, versatilidad y creatividad, mediante el desarrollo de los contenidos, significados, ámbitos, alcances y formas de aplicación del derecho a la protección de datos personales.

La protección de datos personales pertenece al grupo de derechos de la personalidad que tienen como eje común la defensa de la dignidad humana y el libre desarrollo de la personalidad. Por su intermedio se desarrolla el proceso de autoconstrucción de la persona en sociedad y se cristalizan otros derechos como la privacidad, la intimidad, el honor, el buen nombre, la imagen y voz propia, la identidad, entre otros. Asimismo, derechos de larga data,

[560] Ibíd.

como la inviolabilidad del domicilio y sobre de la correspondencia, también pueden ser resguardados directamente por este derecho fundamental, ya que existen nuevos espacios de posible transgresión como, por ejemplo, la geolocalización, la georreferenciación, los correos electrónicos y los sistemas asincrónicos de comunicación que deben ser regulados y en los cuales este derecho puede aportar directamente en el afán de prevenir transgresiones.

La protección de datos personales es un derecho que se convierte en garante de otros derechos, por lo que su efectiva vigencia permite el completar el círculo de protección que incluye entornos virtuales y también físicos. Pero, además, es la autodeterminación informativa el derecho inmanente que lo diferencia de otros derechos de la personalidad, pues otorga un elemento positivo, un derecho acción a favor del individuo en defensa de sus datos y su imagen en sociedad.

Ahora bien, la naturaleza de este derecho, atado a la revolución informática y tecnológica, exige que la respuesta normativa, estatal y ciudadana sea adecuada. Por eso, para garantizar el pleno funcionamiento de este derecho, que permite la defensa integral del individuo, es indispensable una adecuada regulación normativa constitucional y legal que viabilice la ejecución de sus principios propios y sus facultades.

No se debe desconocer que a diferencia de otros países de la región, la protección de los datos personales en Ecuador, paulatinamente ha logrado un reconocimiento constitucional que va completándose, ya que no solo se la considera una garantía, sino que ahora se protege al derecho fundamental.

Sin embargo, en el escenario planteado, es necesaria la tarea del legislador, la del ejecutivo, del jurisdiccional y de los otros poderes del Estado que como generadores de normativa de todo nivel, gestores de políticas públicas y aplicadores, en búsqueda del respeto y garantía de los derechos, construyan un contenido esencial del derecho a la protección de datos personales que permita garantizar la efectiva vigencia del derecho.

Lamentablemente hasta la presente fecha no existe normativa legal que permita un adecuado sistema de prevención y control en el manejo de los datos, sobre todo por parte de los responsables de ficheros privados. En indispensable que se genere una ley específica, una institucionalidad propia y mecanismos de disuasión coercitivos. No son suficientes normativas aisladas y sectoriales, pues mientras más realidades sociales producto de la penetración del internet y las nuevas tecnologías se van incrustando en las realidades sociales del Ecuador, se vuelve indispensable la incorporación de principios y facultades que concreten el ejercicio de este derecho y de otros que, como se vio, están en riesgo.

Entre los principios, la piedra angular es el consentimiento informado, pues solo los datos entregados voluntariamente o por disposición legal, a personas naturales, jurídicas, públicas y privadas pueden ser recopilados, almacenados, manipulados, tratados o cesionados, como materialización de la voluntad de su titular y en ejercicio de sus opciones de vida y manifestación expresa de su perfil en un entorno social. Los otros principios que son intrínsecos de este derecho como, por ejemplo, deber de información, pertinencia, calidad de datos, adecuación del tratamiento a la finalidad autorizada, seguridad, confidencialidad y secreto, permiten además que los datos sean tratados de forma adecuada, pertinente y segura.

Acerca de las facultades propias de este derecho fundamental, en el caso ecuatoriano se efectivizan mediante el *habeas data*; sin embargo, esta garantía constitucional presenta una

evidente limitación: solo procede ante una inminente presencia de daño o ante un daño producido. Una posible solución podría ser una adecuada regulación legal de los principios propios de la protección de datos personales; pero esto sería insuficiente si es que además no se establece un sistema de control y sanción administrativo que disuada a los responsables de las bases de datos o ficheros de cometer transgresiones a los datos personales.

Se podría considerar que la vía penal contemplada mediante el delito de violación a la intimidad, contenida en el artículo 178 del Código Orgánico Integral Penal, es un mecanismo de presión que evite daños; no obstante, el derecho tutelado no es la protección de datos personales, sino la intimidad y, en consecuencia, no existe tipo penal que proteja los datos personales.

Si bien, Ecuador es el primero en configurar el *habeas data reparatorio*; sin embargo, aún prevalecen en nuestros tribunales criterios extraídos del anterior sistema de protección de los datos personales asociados a la intimidad, por lo que esta reparación se limita a mirar el daño únicamente desde la perspectiva de la afectación de este único derecho o a lo sumo del derecho al honor, buen nombre, imagen y propia voz, cuando se evidencia que el uso discriminatorio de datos personales pueden afectar otros derechos fundamentales, y en este sentido, las sentencias deben reparar también los otros derechos vulnerados. Por tanto, se intenta que este carácter reparatorio trascienda del plano económico y se configure como una garantía real que procure la vigencia de todos los derechos afectados.

Se confía en que las continuas reflexiones sobre el desarrollo normativo constitucional del derecho a la protección de datos en Ecuador calen en los poderes estatales, incluida la administración de justicia y permitan un adecuado desarrollo, aplicación y correcta comprensión de las dimensiones crecientes y variantes de este derecho fundamental.

10. Cuadro resumen del contenido esencial del derecho a la protección de datos en Ecuador

ECUADOR					
CONTENIDO ESENCIAL		**NORMA**	**DERECHO A LA PROTECCIÓN DE DATOS PERSONALES**	**NORMA**	***HABEAS DATA***
Dato e información		Constitución (1)	Protege al dato y a la información personal.	Jurisprudencia (*obiter dicta* /no vinculante) (5).	Carácter informativo del dato.
		Constitución	Todo tipo de datos: íntimo, sensible e inocuo.	Ley 2 (3)	La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad; no menciona al derecho a la protección de datos personales porque la vigencia de la ley es anterior a la Constitución que consagra el derecho.
		X	Definición y tipos de datos.	X	*Habeas data* no se refiere a datos e información usa los términos documentos, datos genéticos, bancos o archivos.
		Constitución	Carácter personal del dato.	X	Datos personales e informes sobre sí misma, o sobre sus bienes.
		X	De persona identificada e identificable.	X	X
		X	Tipo de soporte.	Constitución / ley 1 (2)	Soporte material o electrónico.
Titulares		Constitución	Persona natural. Se analizará cada caso particular respecto de persona jurídica, comunidad, pueblo, nacionalidad y colectivo.	Constitución / Jurisprudencia vinculante (4) / ley 1	Personas naturales, jurídicas, comunidades, pueblos, nacionalidades y colectivos. Toda persona.
				Jurisprudencia vinculante	Respecto de personas jurídicas, comunidades, pueblos, nacionalidades y colectivos procede de datos propios y distintos de los miembros, se analizará cada caso.
Objeto o bien jurídico	Derecho de información.	X	X	Constitución / Ley 1	Derecho a conocer de la existencia, finalidad, origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.
	Autodeterminación informativa.	Constitución / Jurisprudencia vinculante.	Decisión sobre información y datos personales.	Jurisprudencia vinculante (4)	La autodeterminación informativa es parte del derecho a la protección de datos personales

	Principio de consentimiento informado	Constitución	Consentimiento del titular no menciona previamente informado.	Constitución / Ley 1	Deber de abstención de difusión de la información, si previamente el responsable del fichero no cuenta con la autorización del titular del dato personal.
	Necesidad de mandato legal para tratamiento sin autorización del titular	Constitución	Mandato legal.	Constitución / Ley 1	Deber de abstención de difusión de la información, si previamente el responsable del fichero no cuenta con la autorización del titular del dato personal o es posible esta mencionada difusión por permitirlo expresamente la ley.
				Ley 1	No podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos.
	Principios	Constitución	Así como su correspondiente protección.	X	X
	Pertinencia	X	X	X	X
	Calidad	X	X	X	X
	Finalidad	X	X	Constitución / Ley 1	Limitado a conocer sobre la finalidad del uso que se haga de los datos.
	Seguridad	X	X	Constitución	Limitado para el caso de datos sensibles.
Contenido de las facultades que les corresponden a los titulares para el ejercicio de ese objeto	Derecho de acceso	Constitución	Acceso sobre información y datos personales .	Constitución / Ley 1	Acceso a documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes.
				Constitución / Ley 1	Acceso sin consto alguno.
	Derecho de rectificación	X	X	Constitución	La persona titular de los datos podrá solicitar al responsable [...] su rectificación.
				Ley 1	Las presentes disposiciones son aplicables a los casos de rectificación a que están obligados los medios de comunicación, de conformidad con la Constitución. Deberá efectuarse una rectificación, réplica o respuesta, en forma inmediata, obligatoria y gratuita, en el mismo espacio u horario en el que se transmitió la información que causó el perjuicio.
				Ley 1	Procede rectificación cuando los datos fueren erróneos o afecten sus derechos.
	Derecho de actualización	X	X	Constitución	La persona titular de los datos podrá solicitar al responsable [...] la actualización de los datos.
				Ley 1	Procede actualización cuando los datos fueren erróneos o afecten sus derechos.
	Derecho cancelación	X	X	Constitución	La persona titular de los datos podrá solicitar al responsable [...] la eliminación o anulación de los datos.

				Ley 1	No podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos.
				X	No hace referencia a cancelación.
	Derecho de oposición	X	X	X	X
	Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales	X	X	Ley 1	Ahora bien, el numeral 3 del artículo 50 de LOGJCC establece que podrá interponerse *habeas data* "cuando se dé un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente".
	Derecho de consulta al registro general de protección de datos personales	X	X	X	X
	Derecho a indemnización por daños causados	X	X	Constitución	La persona afectada podrá demandar por los perjuicios ocasionados.
		X	X	Constitución	El juez resolverá la causa mediante sentencia que [...] ordenará la reparación integral.
		X	X	Constitución / Ley 1	El concepto de reparación integral incluirá todas las obligaciones materiales e inmateriales que el juez determine para hacer efectiva dicha reparación.
Sujetos pasivos u obligados	Responsable del tratamiento	Constitución	Toda persona que recolecte, archive procese, distribuya o difunda datos o información	Constitución / Ley 1	Las personas responsables de los bancos o archivos de datos personales.
				Constitución / Ley 1	Entidades públicas o privadas.
				Ley 1	Entidades públicas o personas naturales o jurídicas privadas.
	Encargado de tratamiento	X	X	X	X
	Tercero	X	X	X	X
	Destinatario	X	X	X	X

Derechos tutelados por el *habeas data*		N/A	N/A	Jurisprudencial vinculante (6)	Protege a la intimidad, la honra, la integridad psicológica de la persona.
				Jurisprudencia no vinculante (5)	Protege a la intimidad, al buen nombre, el honor, la imagen y la propia voz, derecho a la protección de datos personales.
				Ley 1	Derecho de rectificación en medios de comunicación social.
Procedencia *habeas data*		N/A	N/A	Ley 1	Procede *habeas data*: Cuando se niegue el acceso. Cuando se niegue la solicitud de actualización, rectificación eliminación o anulación de datos erróneos o que afecten sus derechos. Cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de juez competente.
				Jurisprudencia vinculante (4)	Legitimado activo debe ser el titular del derecho a la protección de datos personales Acreditada la representación de la persona jurídica no procede excepción de falta de legitimación El *habeas data* no puede invocarse para requerir la entrega física de los documentos que contienen información personal
				Jurisprudencial vinculante (6)	La entidad a quien se requiere el *habeas data* responderá la solicitud efectuada por el titular de la información personal en un plazo razonable. Los criterios que permiten determinar el plazo razonable son: cantidad de información, tipo de pedido, conducta de la entidad a cargo de los datos personales. Calificación de la razonabilidad deberá realizarla el juez. La falta de contestación de la entidad a cargo de los datos personales se considera negativa tácita a la solicitud de acceso presentado por el titular y habilita presentar habeas data.
Procedimiento de *habeas data*	Procedimiento previo	N/A	N/A	Ley 1	La persona titular de los datos podrá solicitar al responsable sin costo el acceso, la actualización, rectificación, eliminación o anulación.
	Acción constitucional	N/A	N/A	Constitución / Ley 1	Si la solicitud no fuere atendida podrá acudirse al juez de primera instancia que actúa como juez constitucional mediante *habeas data*.
	Apelación	N/A	N/A	Constitución / Ley 1	La sentencia de primera instancia podrá ser apelada ante la Corte Provincial.
	Jurisprudencia vinculante	N/A	N/A	Constitución / Ley 1	Las sentencias ejecutoriadas serán remitidas a la Corte Constitucional, la cual por medio de la Sala de selección escogerá aquellas que permiten desarrollar el sistema de precedentes jurisprudenciales.

	Resolución vinculante (consulta de norma)	N/A	N/A	Jurisprudencial vinculante (7)	Para procesos de *habeas data*, se debe aplicar de forma supletoria, el Capítulo III Sobre Excusa y Recusación del Código General de Procesos
Institucionalidad de protección		X	X	X	X
Régimen sancionador		X	X	Constitución / Ley 1	Reparación integral.
Transferencia internacional de datos		X	X	X	X

1. *Constitución de la República del Ecuador* [2008], en RO, No. 449 (20 de octubre de 2008).
2. Ecuador, *Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional*, Ley 0, en ROS, No. 52 (22 de octubre de 2009).
3. Ecuador, *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*, Ley 67, en ROS, No. 557 (17 de abril de 2002).
4. Ecuador, Corte Constitucional del Ecuador, [Sentencia No. 001-2014-PJO-CC], en ROS, No. 281 (3 julio de 2014). Sentencia vinculante.
5. Ecuador, Tribunal Constitucional del Ecuador, [Sentencia No. 0070-2003-HD], RO, No. 271 (11 febrero de 2004 / 22 de diciembre de 2003). Sentencia no vinculante.
6. Ecuador, Corte Constitucional del Ecuador, [Sentencia No. 00182-15-SEP-CC], en ROS, No. 596 (28 de septiembre de 2015).
7. Ecuador, CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 006-17-SCN-CC], en ROEC, No. 22 (05 de diciembre de 2017).

Tabla elaborada por la autora (2019).

CAPITULO II

RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES EN EL MODELO EUROPEO

1. Justificación de la protección de la información y de los datos personales

A partir del siglo XX nos desarrollamos en un universo de comunicación y tecnología, el cual ha motivado un cambio en las estructuras jurídico-económicas similar al producido con la revolución industrial. La información constituye el eje central del sistema[561], aquel poder, que dirigido de manera positiva propende al desarrollo económico, cultural y tecnológico de los pueblos y que ha permitido el nacimiento de la sociedad de la información y de su radicalización, a través de la hiperconexión, el vertiginoso procesamiento de grandes volúmenes de información y la implementación de una estructura social globalmente interdependiente, cualidades propias de la sociedad red.[562]

La problemática inherente del uso de las nuevas tecnologías pone a prueba la capacidad de los profesionales y académicos del derecho para entregar respuestas a los efectos y cambios que se producen a escala nacional e internacional. La multiplicación de nuevas tecnologías de la información y la comunicación, aplicables en los distintos ámbitos de la vida de las personas ha puesto en riesgo la dignidad humana y los derechos que permiten el libre desarrollo de la personalidad.

En ese escenario, toma vital importancia la protección de la información,[563] sobre todo de aquella de carácter personal que aparece en el diario trajinar del individuo en sociedad y más aún en el ciberespacio, administradas tanto por entidades públicas como privadas.

Originalmente, las leyes se limitaban a regular y sancionar aquellas transgresiones de derechos fundamentales, relativas a la difusión incompleta, inexacta y lesiva de información vertida a través de medios de comunicación tradicionales (diarios, radios, televisión, revistas) y nada mencionaba respecto de aquella contenida en medios digitales o en el mundo virtual, aun cuando, a diferencia de la analógica, los actuales "recursos tecnológicos no conocen el olvido, ni se detienen ante la lejanía y son capaces de

[561] "La sociedad postindustrial informatizada se acoge a un modelo de organización socioeconómica que se basa en la producción y transmisión de informaciones. A la sociedad informatizada la definen los bancos de datos y las redes de información." C. CONDE ORTIZ, *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad* (Madrid: Dykinson S.L., 2005), 16.

[562] M. CASTELLS y F. MUÑOZ DE BUSTILLO, *La sociedad red: Una visión global* (España: Alianza Editorial, S.A., 2013), 73.

[563] Información: "5. f. Comunicación o adquisición de conocimientos que permiten ampliar o precisar lo que se posee sobre una materia determinada". Diccionario de la Lengua Española, http://dle.rae.es/?id=LXrOqrN. Con base en los datos precedentes -Juan-, -1970-, -35-, se dispondría de una información determinada: Juan, nacido en el año 1970, tiene 35 años, etc. La mayoría de legislaciones como la española protegen, bajo el título de datos personales "cualquier información concerniente a personas físicas identificadas o identificables". I. LÓPEZ VIDRIERO TEJEDOR y E. SANTOS PASCUAL, *Protección de Datos Personales: Manual Práctico para Empresas* (Madrid: Fundación Confemetal Editorial, 2005), 29.

almacenar, relacionar y comunicar en tiempo real ingentes masas de datos de todo tipo, incluidos los de carácter personal y de utilizarlos para las más diversas finalidades".[564] Así, la tecnología ha superado los límites que antes condicionaban el tratamiento de información de esta naturaleza, pues permiten aplicar una serie de sistemas de almacenamiento, identificación, ciframiento, análisis, etc.

Es agobiante pensar que se pueda reconstruir a un individuo en prácticamente todos los aspectos de la vida, a partir de lo que podríamos pensar son informaciones inofensivas y carentes de interés, lo cual nos lleva a pensar en lo vulnerable de nuestra privacidad frente a las nuevas tecnologías y en la posibilidad de que las conclusiones de estas reconstrucciones sean equivocadas. "Todo ello pone en manos de quien lo hace un poder de control sobre los afectados -que potencialmente lo somos todos- que merma su libertad, identidad e, incluso, dignidad".[565]

El titular del dato ha perdido el control de su propia información y es obligación del Estado devolverle este poder para garantizarle derechos fundamentales y la protección de sus datos personales, por medio de la concreción de este derecho desde una visión preventiva, así como ulterior mediante la aplicación de mecanismos de garantía y defensa de su autodeterminación informativa.

2. Sistemas de protección de datos personales

A escala mundial es perceptible la problemática de los datos personales, ya sea desde una visión antigua acotada a la intimidad[566] o sesgada limitada a la privacidad,[567] o desde una perspectiva autónoma que reconoce en la naturaleza misma del dato personal,[568] la necesidad de su salvaguarda, esto es por su condición de identificar o hacer identificable a una persona, independientemente de si tiene el carácter de íntimo o privado.

En consecuencia, no existe un sistema único de protección, ya que cada ordenamiento jurídico encara de forma distinta esta realidad, siendo las más comunes las siguientes:

a) Mediante normas generales, de carácter constitucional o legal, nacional o internacional,[569] a través de las cuales se establecen principios generales de carácter obligatorio e incluso en muchos casos de aplicación directa.

[564] P. MURILLO, "Diez preguntas sobre el derecho a la autodeterminación informativa y la protección de datos de carácter personal", *Agencia Catalana de Protección de Datos*, 13 de enero de 2006, www.apd.cat..

[565] Ibíd.

[566] Varios países latinoamericanos aún protegen los datos personales desde la limitada visión de la intimidad, pues no reconocen un derecho autónomo o independiente, estos son: Bolivia, Chile, Guatemala, Honduras, El Salvador, Paraguay y Venezuela.

[567] Modelo anglosajón por el cual se protege a las personas y sus datos desde la perspectiva de la *privacy*.

[568] Modelo europeo que reconoce el derecho a la protección de datos personales.

[569] Los instrumentos internacionales globales o regionales cumplen la finalidad de ser normas de carácter general y aún más permiten la unificación legislativa y la aplicación uniforme sobre todo en lo relativo al flujo de datos transfrontera.

b) Mediante normas específicas y sectoriales de protección de datos, que tratan aspectos concretos y que pueden ser de carácter legal o reglamentario,[570] como por ejemplo leyes especiales.
c) Mediante la adopción de códigos de conducta deontológicos o de ética y los contratos-acuerdo, es decir aquellos que reciben la aprobación de un organismo público que ejerce el poder de control en materia de protección de datos; se usan mayormente en transferencias internacionales de datos que resuelve la falta de estándares nacionales equivalentes, en casos de determinados objetos del contrato.[571]
d) Mediante las reglas del mercado, el tratamiento de datos sometido a las reglas de la economía, es decir vía protección contractual, sujeto a la autonomía de la voluntad.[572]

Como formas de tutela efectivas, que garantizan el derecho de los registrados a acceder, modificar, eliminar, etc. los datos personales, se ha implementado las siguientes:

a) La garantía constitucional que se la conoce como *hábeas data* y que permite el acceso, la modificación y eliminación de datos de carácter personal, generalmente reconocida en Latinoamérica;
b) Los recursos ante el órgano de control y otras vías administrativas, tales como recursos de amparo o de tutela emergente; y,
c) Las acciones judiciales.

Sin embargo, existe una tendencia mayoritaria que marca la necesidad de la homogeneización y armonización de las regulaciones por medio de la determinación de principios y criterios coincidentes que faciliten las interrelaciones comerciales, industriales, financieras, etc. entre los

[570] Como la Ley de Burós de Créditos o los convenios en los que las partes establezcan el manejo de los datos de carácter personal y las sanciones por su incumplimiento.
[571] M. EKMEKDJIAN y C. PIZZOLO, *Hábeas data: el derecho a la intimidad frente a la revolución informática* (Buenos Aires: Ediciones Depalma, 1996).
[572] "Si bien, La Landtag de Hesse de 1970 la *Privacy Act* de 1974, primeras normas con un relativo contenido a la protección de datos solo vinculan a los poderes públicos, pues en su momento fracasaron los intentos de extender el ámbito de aplicación de la ley al sector privado. Sin embargo, "gradualmente el estado ha ido implementando controles sobre el manejo de la información esto en razón de un evento devastador, los atentados terrorista del 11 de septiembre de 2001, que provocaron una reacción legislativa represiva en aras de proteger a los estados de ataques. En tal virtud se dictan normas como la USAPA o Patriotic Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) mediante la cual se autorizó a las agencias de seguridad e inteligencia a inmiscuirse en aspectos privados de las personas e incluso acceder a datos de carácter personal, ingresando en las comunicaciones realizadas por Internet, rastreando destinos, analizando contenidos de operaciones comerciales, cuentas bancarias, tarjetas de crédito, correos electrónicos etc., con escaso o nulo control judicial, los controles migratorios estrictos que incluyen la obtención y registro de datos de carácter personal de los viajeros internacionales. Esta obsesión por el control de algún modo comenzó a expandirse tanto en Europa por los atentados sufridos por España el 11 de marzo del 2004 como en América Latina por Colombia y su guerra antiterrorista y Argentina y resto de países por el innovador secuestro express." O. PUCCINELLI, "Tipos y subtipos de hábeas data en América Latina", *Editorial Astrea*, 2004, accedido 8 de junio de 2007, http://www.infobaeprofesional.com/adjuntos/documentos/08/0000887.pdf

Estados, mediante la transmisión de datos internacionales, esto es diseñar un sistema adecuado, universal y unificado.

3. Paulatina configuración del derecho a la protección de datos personales

Acorde con la realidad imperante se vuelve indispensable establecer una protección jurídica completa que observe lo relativo a los datos de carácter personal[573] y a las bases que los contienen, a su acceso, almacenamiento, registro sistemático, elaboración, difusión y transmisión completa y que permita evitar la transgresión de toda clase de derechos fundamentales, entre ellos, la intimidad, la privacidad, el honor, la imagen y la voz de la personal y la autodeterminación informativa.

La forma en la que el derecho ha respondido a esta realidad es mediante la formulación de un nuevo derecho con contenido y reglas propias, denominado el derecho a la protección de datos. Entiéndase que su finalidad real no es la protección de datos, sino la protección de las personas, titulares de esos datos.

Originalmente, este derecho nace en el ámbito de la intimidad o de la *privacy* anglosajona, pues por su intermedio se protegían aquellos datos que reflejan aspectos de la esfera íntima o privada de una persona.

Finalmente, la realidad tecnológica desbordó esta defensa inicial, pues se comprobó que incluso aquellos datos considerados en principio irrelevantes, porque no afectan a la intimidad, podían ser usados para conculcar otros derechos fundamentales, como el derecho al trabajo, a la salud, a la vivienda, a la educación, etc.

Por lo tanto, la protección debió ser ampliada, no limitarse a los datos íntimos o privados sino a todos los datos de un individuo, no solo al control de la intimidad del individuo sino al control sobre todos sus datos. Efectivamente, aquí nace el derecho a la autodeterminación informativa cuya sustantividad ya no es la intimidad o la privacidad, sino el derecho de las personas a controlar toda su información cualquiera sea su naturaleza.

De todo lo dicho, se puede concluir entonces que la protección de datos personales es:

> [...] la garantía de la libertad informática, como derecho a controlar el uso de los datos insertos en un programa informático, el *hábeas data*, es decir el derecho del afectado a consentir sobre la recogida, uso de datos y a saber de los mismos [...] se constituye un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es,

[573] Dato, según el Diccionario de la Lengua Española, es el "antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencia legítimas de un hecho". Por dato se podría considerar un nombre -Juan-, un año -1970-, un número-35, etc. I. LÓPEZ-VIDRIERO y E. SANTOS PASCUAL, *Protección de Datos Personales, Manual Práctico para Empresas*.

> en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones al dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos.[574]

En suma, un derecho que evita la discriminación producida por inadecuadas valoraciones automatizadas o por imprecisiones de la información personal contenida en bases de datos. Un derecho que protege el libre desarrollo de la personalidad, garantiza el ejercicio de otros derechos de la personalidad, permite el proceso de autoconstrucción de un individuo en sociedad y genera personas libres, informadas y empoderadas que contribuyen a la construcción de un Estado democrático.

4. Autodeterminación informativa, un derecho fundamental de formación jurisprudencial en el modelo europeo

El origen jurisprudencial del derecho a la protección de datos se sitúa en la sentencia del 15 de diciembre de 1983, dictada por el Tribunal Constitucional Federal Alemán.[575] En ella se declaró parcialmente inconstitucional la ley de censo demográfico, de 25 de marzo de 1982, que obligaba a los ciudadanos germanos a suministrar datos personales para fines estadísticos, por cuanto se excedía en las informaciones que se les solicitaban. Dicha sentencia establece que el derecho a la autodeterminación informativa consiste en la "facultad del individuo de decidir, básicamente, cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida, haciendo necesaria la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitadas de los datos concernientes a la persona".[576] El titular, no tiene un señorío ilimitado sobre sus datos personales, no solo por ser parte y desarrollarse dentro de una organización social basada en la comunicación de sus individuos, sino porque este derecho no es absoluto, pues debe ponderarse con otros bienes jurídicos para garantizar un interés general o superior. Ahora bien, por tratarse de un derecho es indispensable un fundamento constitucional o legal que establezca sus límites.[577]

En España, por su parte, la primera sentencia relativa a la protección de datos es la STC 254/1993, de 20 de julio, respecto de un recurso de amparo promovido por Foz en contra de la denegación presunta del Gobernador Civil de Guipúzcoa y del Ministro del Interior, de la solicitud de información relativa a la existencia, finalidad y responsables de los ficheros automatizados, de los datos de carácter personal que constaban en los ficheros

[574] Perú: TRIBUNAL CONSTITUCIONAL, [Sentencia 254/1993], Sistema HJ, accedido 11 de abril de 2018, http://hj.tribunalconstitucional.es/it/Resolucion/Show/2383.
[575] Alemania: TRIBUNAL CONSTITUCIONAL FEDERAL, [Sentencia de 15 de diciembre de 1983, BJC n.º 33, IV Jurisprudencia Constitucional Extrajera], 1984.
[576] C. RUIZ, *El derechos a la protección de la vida privada en la Jurisprudencia del Tribunal Europeo de Derechos Humanos* (Madrid: Cuaderno Civitas, 1994), 50.
[577] H. RUDOLF, ed., *Jurisprudencia del Tribunal Constitucional Federal Alemán, Extractos de las sentencias más relevantes compiladas por Jürgen Schwabe* (México, DF.: Konrad Adenauer Stiftung e. V, 2009), 94, accedido el 20 de octubre de 2019, http://www.kas.de/wf/doc/kas_16817-544-4-30.pdf.

automatizados de dicha Administración.[578] En su parte pertinente, dicha sentencia señala que:

> Dispone el artículo 18.4 CE que «la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». De este modo, nuestra CE ha incorporado una nueva garantía constitucional como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo de tratamiento mecanizado de datos, lo que la CE llama «la informática».

En suma, la sentencia señala por primera vez la existencia de un derecho emancipado del derecho a la intimidad y específico con sustantividad propia, pues garantiza la protección de los datos personales, es decir el derecho de control que tienen los ciudadanos sobre sus datos.

Una sentencia de marcada importancia es la STC 124/1998, de 15 de junio, dentro del procedimiento de tutela de los derechos fundamentales de un trabajador de la empresa RENFE contra esta. El trabajador estaba afiliado al sindicato "Comisiones Obreras", el cual convocó a una huelga, a la que el peticionario no pudo acogerse debido a su horario laboral. Sin embargo, al recibir su nómina correspondiente al mes de mayo de 1994, RENFE le retuvo una cantidad, motivada en su supuesta participación en los paros del mes anterior. Ante el reclamo del peticionario, la empresa reconoce su error y devuelve la cantidad. Sin embargo, RENFE utilizó un dato que pertenecía a la privacidad del trabajador, y que lo poseía con la finalidad exclusiva de descontar la cuota de filiación sindical, y no para impartir instrucciones al sistema informático a fin de que se descuenten, de aquellos que tienen clave 893 correspondientes a los afiliados al mencionado sindicato, de todos los días de paro en los que supuestamente participó. En consecuencia, RENFE es sancionada por la violación del derecho fundamental a la autodeterminación informativa. Anótese que esta sentencia es fundamental para el desarrollo del derecho a la protección de datos, pues marca su decisivo nacimiento, ya que afirma que el artículo 18.4 CE consagra un derecho fundamental autónomo e independiente de controlar el flujo de informaciones que le conciernen a cada persona, para así preservar el pleno ejercicio de otros derechos como lo fue en este caso el laboral.[579]

[578] Perú: TRIBUNAL CONSTITUCIONAL, [Sentencia 254/1993].
[579] España: TRIBUNAL CONSTITUCIONAL, [Sentencia 124/1998], Sistema HJ, accedido 11 de abril de 2018, http://hj.tribunalconstitucional.es/cs/Resolucion/Show/3626.

Otra sentencia fundamental es la STC 202/1999, de 8 de noviembre,[580] motivada por la reclamación que hace un empleado a una entidad crediticia, para que le sea informado de la existencia, finalidad y contenido de una base de datos en la que constaban su absentismo por baja médica. Dicha sentencia, en su parte resolutiva, trae a colación si la tutela frente al tratamiento de los datos personales se logra mediante el derecho a la intimidad o por medio de un derecho fundamental nuevo y diverso denominado "autodeterminación informativa". En la parte pertinente dice:

> Se trata por tanto, de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a potenciales agresiones a la dignidad y a la libertad de las personas provenientes de un uso ilegítimo del tratamiento mecanizado de datos… la «llamada libertad informática» es así el derecho a controlar el uso de los mismos datos insertos en un programa (*hábeas data*) y comprenden entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos a aquel legítimo que justificó su obtención.

En esta sentencia es relevante destacar la conceptualización de "la libertad informática" como aquel derecho que tienen todas las personas a decidir que espacios de su libertad ceden; es decir, qué datos, en qué condiciones y con qué finalidades desean facilitarlos.

La sentencia que permite el reconocimiento del derecho a la autodeterminación informativa como un derecho fundamental es la SSTC 290/2000, de 30 de noviembre, en la que se discute la competencia de las agencias de protección de datos CCAA, entre el Gobierno y el Parlamento de Cataluña, a raíz de la publicación de la LORTAD.[581] La Comunidad Autónoma consideraba que el artículo 18.4 de la Constitución no contenía en sí mismo un derecho fundamental, sino una vía de limitación del uso de la informática. Por lo tanto, que las agencias de protección de datos CCAA tenían competencia para controlar y registrar los ficheros de titularidad privada radicados en su territorio cuando el ámbito material en el que estos operan sea de materias de competencia de las Comunidades Autónomas. Ante esta afirmación, el Tribunal Constitucional señaló que el artículo 18.4 establece un derecho fundamental, el de la protección de datos personales y que, por lo tanto, la competencia corresponde a la Agencia Española de Protección de Datos que, por su carácter estatal, es la encargada de velar su vigencia.

Podríamos citar muchas otras sentencias que han construido el derecho a la protección de datos, pero finalmente queremos recoger a manera de colofón, la sentencia 292/2000, de 30 de noviembre,[582] que supone de forma definitiva el reconocimiento de un derecho

[580] España: TRIBUNAL CONSTITUCIONAL, [Sentencia 202/1999], Boletín Oficial Español, accedido 11 de abril de 2018, https://www.boe.es/boe/dias/1999/12/16/pdfs/T00019-00026.pdf.
[581] España: TRIBUNAL CONSTITUCIONAL, [Sentencia 290/2000], Boletín Oficial Español, accedido 11 de abril de 2018, https://www.boe.es/buscar/doc.php?id=BOE-T-2001-330.
[582] España: TRIBUNAL CONSTITUCIONAL, [Sentencia 292/2000], Boletín Oficial Español, accedido 11 de abril de 2018, https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332.

autónomo, distinguiéndolo del derecho a la intimidad, porque este último no permite una protección suficiente ante la realidad derivada del progreso tecnológico. La sentencia en su parte más relevante dice:

> Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 18.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.
> 6. La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144 (1999, de 22 de julio, FJ 8)".[583]

Se "impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidos de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin".[584]

Entonces, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno; por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5;[585] 144/1999, FJ 8; 98/2000,[586] de 10 de abril, FJ 5;[587] 115/2000, de 10 de mayo, FJ 4);[588] es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos.

---

[583] España: TRIBUNAL CONSTITUCIONAL, [Sentencia 144/2003], Sistema HJ, accedido 11 de abril de 2018, http://hj.tribunalconstitucional.es/es/Resolucion/Show/4919.
[584] España: TRIBUNAL CONSTITUCIONAL, [Sentencia 292/2000].
[585] España: TRIBUNAL CONSTITUCIONAL, [Sentencia 134/1999], Sistema HJ, accedido 11 de abril de 2018, http://hj.tribunalconstitucional.es/eu/Resolucion/Show/3876.
[586] España: TRIBUNAL CONSTITUCIONAL, [Sentencia 144/2003].
[587] España: TRIBUNAL CONSTITUCIONAL, [Sentencia 98/2000], Sistema HJ, accedido 11 de abril de 2018, http://hj.tribunalconstitucional.es/gl/Resolucion/Show/4082.
[588] España: TRIBUNAL CONSTITUCIONAL, [Sentencia 115/2000], Sistema HJ, accedido 11 de abril de 2018, http://hj.tribunalconstitucional.es/it/Resolucion/Show/4099.

5. Evolución y armonización de la protección de datos: declaraciones, convenios y directivas

Europa es la cuna del derecho a la protección de datos personales; además, está a la vanguardia de un estatus de protección adecuado que permita el libre flujo informacional y la garantía de los derechos fundamentales de los ciudadanos. Esta afirmación se debe a la reciente emisión del Reglamento General del Protección de Datos Personales dictado en el año 2017 y que entró en vigencia el 25 de mayo de 2018, que deberá ser aplicado de forma directa por cada uno de los países miembros sin necesidad de adaptación previa de su normativa interna.

Para comprender la evolución de este sistema de protección de datos personales es necesario identificar cómo se ha producido la paulatina armonización de la jurisprudencia y de la normativa europea. A continuación, desde una perspectiva histórica, en orden cronológico, se desarrollará los antecedentes normativos que han permitido marcar una homologación de conceptos, objetivos y presupuestos de protección que han vislumbrado el camino para la promulgación del actual Reglamento europeo.

5.1 Primeras iniciativas: del derecho a la intimidad y la *privacy* a la protección de datos personales

Las primeras iniciativas que delinearon el derecho a la intimidad, surgieron ante la necesidad de ponderar dos derechos fundamentales, el derecho a la información o libertad de prensa y el derecho a la intimidad, que en el derecho anglosajón se conoce como *privacy*. "Será en la segunda mitad del siglo XIX, cuando generalizada la burguesía y convertida ésta en clase social dominante, propiedad e intimidad se separan; la intimidad deja de ser un derecho perteneciente a una clase social con un sentido patrimonial. Este concepto se atribuye a los juristas *Warren y Brandeis*[589] nacido en un famoso artículo llamado «*The right to privacy*» que publicaron en la «*Harvard Law Review*», el 15 de diciembre del año 1980, en el que trataron de argumentar el derecho a ser dejado sólo de carácter subjetivo, en el sentido de excluir a los demás del conocimiento de noticias, especialmente frente a la prensa".[590]

[589] "Conviene advertir, a fin de situar en su justo contexto el trabajo pionero de Warren y Brandeis, que su origen no fue del todo «heroico». El motivo, que despertó la imaginación de Warren y le indujo a recabar la colaboración de su antiguo compañero de estudios, Brandeis, para realizar el artículo, distaba mucho de ser altruista y desinteresado. En concreto Warren, que tras su matrimonio con la hija del senador Bayard, de una prestigiosa familia de Boston, conducía una vida privada dispendiosa y desordenada, deseaba verse libre del asedio de la prensa. Se perseguía, en suma dejar a salvo a la alta burguesía de las críticas e indiscreciones de la prensa". A. MILLAR, "The Assault on Privacy", *The University of Michigan Press*, Ann Arbor, 1971: 185 ss., accedido 16 de junio del 2007, http://portal.acm.org/citation.cfm?id=1017625.1017632&coll=GUIDE&dl=GUIDE&CFID=442837&CFTOKEN=90223178

[590] M. SERRANO, *El derecho fundamental a la protección de datos: derecho español y comparado* (Madrid: Thomson Civitas, 2002), 29.

El análisis realizado por los autores es sin duda empírico, basado en la experiencia que Samuel D. Warren había percibido tras casarse en 1883 en Washington, D. C. con la Mabel Bayard, hija del senador Thomas Bayard. A partir de ese suceso, Warren comenzó a sentirse acosado por la prensa que no dudaba en publicar hasta los más mínimos detalles de su vida.

El día de su boda todos los medios cubrieron la ceremonia y la fiesta. De tal relevancia fue dicho acontecimiento que hasta reconocidos diarios como el Washington Post y el New York Times dedicaron planas enteras a comentar sobre cada uno de los aspectos que se llevaron a cabo ante tan notado suceso. A partir de ese día, tanto él como toda su familia, hasta el primo más lejano, eran perseguidos constantemente por *paparazzis*; las bodas de cualquier conocido, amigo o familiar eran cubiertas y los chismes acerca de su matrimonio crecían con gran velocidad.[591]

Las circunstancias bajo las que se encontraba lo hacían sentir molesto, sus amigos y familiares se apreciaban constantemente incómodos. La impresión de estar vigilados 24 horas, los 7 días de la semana agotaban la paciencia del abogado Warren. Años después, junto con su amigo y colega Brandeis, decidió ponerle fin a esa persecución y empezar a buscar dentro de la legislación y jurisprudencia estadounidense una solución ante tales intromisiones.

Dentro del citado artículo se buscaba una solución jurídica al conflicto que se había planteado acerca de la intromisión a la privacidad de las personas, se pretendía que cualquier criterio esté orientado a la protección de la dignidad humana y no solo se atienda a la propiedad privada.[592]

Entonces, el mayor avance de la conceptualización del derecho a estar solo, a ser dejado en paz, «*the right to be alone*», es el de considerarlo un derecho autónomo e independiente del concepto de propiedad, ya que hasta entonces se lo tenía estrechamente vinculado como "condición para acceder a la intimidad",[593] pues solo quien tenía propiedades (casa) podía desarrollar un espacio de privacidad. La intimidad era considerada un privilegio de la naciente burguesía en la revolución industrial y, por ello, su nacimiento que "cronológicamente coincide con la afirmación revolucionaria de los derechos del hombre, no supuso en la sociedad burguesa la realización de una exigencia natural de todos los hombres, sino la consagración de privilegio de una clase".[594]

---

[591] A. GAJDA, "What if Samuel D. Warren Hadn't Married a Senator's Daughter?: Uncovering the Press Coverage that Led to The Right to Privacy", *Michigan State Law Review*, n.º 1 (2008), accedido 17 de octubre de 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1026680.

[592] Ibíd.

[593] A. M. BENDICH, Privacy, "Poverty and the Constitution", *Conference on the Law of the poor* (Berkeley: University of California, 1966), 7, accedido 16 de junio del 2007, http://links.jstor.org/sici?sici=0008-1221(196605)54%3A2%3C407%3APPATC%3E2.0.CO%3B2-9

[594] S. RODOTA, *La privacy tra individuo e collettivitá*, accedido 16 de junio de 2007, http://www.emsf.rai.it/grillo/trasmissioni.asp?d=607

Aunque su creación tuvo un origen de naturaleza privada e individualista, paulatinamente, el desarrollo de la sociedad, sobre todo por la aparición de la tecnología y las comunicaciones, aun de las incipientes, motivó a que se marcase un avance, pues su significación debió tornarse pública-colectiva, tanto más que la mayoría de las agresiones que la intimidad sufre se producen en la dimensión social del ser humano.

Así, el primer antecedente normativo se lo encuentra en el artículo 12 de la Declaración Universal de los Derechos Humanos, proclamada por la Asamblea General de la ONU, el 10 de diciembre de 1948, por el cual se consagra a la intimidad como un derecho fundamental del hombre, al señalar que se debe proteger a toda persona ante injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, así como de ataques contra su honra y reputación.

Entonces, era evidente que los principales instrumentos a escala internacional incluyeran el derecho a la intimidad dentro de sus textos junto con otros derechos de estrecha vinculación como el derecho a la honra, reputación y la inviolabilidad de correspondencia. Esto es en la Declaración Americana de Derechos y Deberes del Hombre de 1948 (art. V), como en el Pacto de San José de 1966 relativo a los Derechos Civiles y Políticos, y en la Convención Americana de 1969, que determina la existencia del derecho a la protección de la vida privada como derecho fundamental del hombre.

Este conjunto de Declaraciones por reconocer a la intimidad o la privacidad como derecho fundamental se citan obligatoriamente como antecedentes del derecho a la protección de los datos, porque permiten clarificar la evolución paulatina de los límites de identidad de cada uno de estos derechos.

En el sistema europeo de protección, el derecho a la intimidad fue reconocido por primera vez en el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, de Roma, el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. Cuyo texto señala expresamente:

> Derecho al respeto a la vida privada y familiar 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Es decir, además de reconocer el derecho a la intimidad hace alusión expresa a la prohibición de injerencia de la autoridad pública a esta esfera privada, a menos que la ley lo autorice.

Sobre la base de la citada norma, Europa reconoce en el derecho a la intimidad una primera forma de protección de la persona y su dignidad respecto de los adelantos y usos de las tecnologías de la información y comunicación. Pero, es para 1967 que el Consejo de Europa decide convocar a una comisión consultiva que estudie las tecnologías de la información y su influencia sobre los derechos de las personas y en la cual se concluyó en la necesidad de un marco de protección adecuado para la información de carácter personal que refleja la intimidad de la persona. La finalización de estos trabajos trajo consigo la Resolución 68/509/CE sobre derechos humanos y nuevos logros científicos y técnicos,[595] cuya finalidad fue emitir un pronunciamiento respecto de la necesidad de proteger la privacidad frente a las nuevas tecnologías.

El derecho a la intimidad se evidenció al ponderarlo con el derecho a la información o libertad de prensa; sin embargo, su mayor vulneración se produce a partir de la década de 1960, por el devenir tecnológico, con la aparición de las computadoras y el desarrollo de las autopistas de la información,[596] esto es de las redes digitales, y en los últimos años de la red de redes, internet. La circulación masiva de datos que pertenecen al espacio de intimidad de cada individuo, es decir que tienen el carácter de personales, su almacenamiento y tratamiento diverso, pone de manifiesto la transgresión de este derecho.

Para 1973, el Comité de Ministros del Consejo de Europa dictó la Resolución 73/22, relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado. Un año después expidió la Resolución 74/29, relacionada con la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público.

Por su parte, Estados Unidos, con la Privacy Act de 1974, dictó las primeras normas relativas a protección de la *privacy*, aunque solo referidas a los datos que maneja el Estado. Posteriormente, en 1977, Suecia expidió la *Datalag* que:

> [...] somete a la obtención de autorización previa la creación de bancos de datos, prohíbe el procesamiento de juicios de valor sobre las personas e instituye una inspección de datos, integrada por parlamentarios y representes de la administración para vigilar el uso de la informática en el campo de las informaciones personales, ejerciendo una influencia en Europa. De este modo otros *Länder* aprobaron sus respectivas leyes y se elaboró la *Bundesdatenschutzgesetz*. Esta última se distingue porque no se limita a regular la

[595] CONSEJO DE EUROPA, *PACE - Recommendation 509 (1968) - Human rights and modern scientific and technological developments,* accedido 23 de abril de 2018, http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?FileID=14546&lang=EN.
[596] H. CAMPUZANO, *Vida privada y datos personales* (Madrid: Editorial Tecnos, 2000), 66

> protección de datos en el sector público, sino que, además disciplina la utilización informática de datos personales por parte de empresas privadas.[597]

Posteriormente, en Francia con la *Loi* 78-17 *du 6 janvier, relative a l'informatique. Aux fichiers et aux libertés*, se otorgaron derechos de acceso y control y se constituyó la Comisión Nacional de la Informática encargada de verificar su vigencia.

Finalmente, en Portugal, en el artículo 35 de su Constitución de 1976, se señaló claramente el derecho de acceso a registros mecanográficos, a conocer su finalidad, a rectificarlos, actualizarlos, a la prohibición de tratamiento de datos sensibles y de atribución de un número nacional único a los ciudadanos.

Dentro del derecho británico es la *Data Protection Bill* de 1997 y *Data Protection Act* de 1998, Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal los que regulan, sobre todo, la recogida y circulación de datos de carácter personal.

5.2 Europa y la protección de los datos personales

De vuelta en el espacio europeo, y a fin de evitar las transgresiones del derecho a la intimidad, sobre todo acerca de su relación con las tecnologías de la información, se realizaron grandes esfuerzos por concertar distintas posiciones en materia de protección de datos personales, por intermedio de organismos regionales, que han permitido la elaboración de varia normativa internacional dictada por la Asamblea del Consejo de Europa, el Consejo de la Organización de Cooperación y Desarrollo Económico, y el Consejo y el Parlamento de la Unión Europea, que la regulan y establecen directrices a seguir por parte de los países miembros, a fin de que su legislación interna esté acorde con las normas comunitarias.

La Organización de Cooperación y Desarrollo Económico dictó una Recomendación del Consejo, de 1 de octubre de 1980, relativa a los *Flujos Transfronterizos para el Desarrollo Económico y Social*, cuyo propósito era impedir que los datos recogidos o tratados en un Estado salgan de un territorio a otro que no tenga legislación con mínimos de protección; es decir, la protección de los datos pero referido a su libre tránsito por su utilidad económica.

El Consejo de Europa expidió el Convenio 108/81 CE, de 28 de enero de 1981, *para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, que no tenía carácter vinculante, y que se refería a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en una faceta más profunda porque su motivación inicial ya no es la libre circulación de datos, sino la protección en sí misma de aquellos valores fundamentales como el respeto a la vida

[597] P. LUCAS MURILLO, *El derecho a la autodeterminación informativa* (Madrid: Editorial Tecnos, 1990), 131.

privada. Asimismo, la Comisión dictó la Recomendación 81/679/CEE, de 29 de julio de 1981, sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, DOCE n.º L 246, de 29 de agosto de 1981.

En la década de 1980, el Comité de Ministros del Consejo de Europa ha expedido diversas recomendaciones: (1983) Recomendación 83/10, relativa a la protección de los datos de carácter personal utilizados con fines de investigación científica y de estadísticas; (1985) Recomendación 85/20, relacionada con la protección de los datos de carácter personal utilizados con fines de mercadeo directo; (1986 Recomendación 86/1, relativa a la protección de datos de carácter personal utilizados con fines de seguridad social; (1987) Recomendación 87/15, que regula la utilización de datos de carácter personal en el sector de la policía; (1989) Recomendación 89/2, sobre protección de los datos de carácter personal utilizados con fines de empleo.

En 1990, la Comisión de la Comunidad Europea, emitió la comunicación sobre protección de las personas en lo referente al tratamiento de datos personales y a la seguridad de los sistemas de información. En 1991, el Comité de Ministros del Consejo de Europa dictó la Recomendación 91/10 sobre la comunicación a terceros de datos de carácter personal en poder de organismos públicos. En 1994, la Comisión del Consejo de Europa expidió la Recomendación 94/820/CE, relativa a los aspectos jurídicos del intercambio electrónico de datos, DO L 338 de 28.12.1994, pp. 98-117. Para 1995, el Comité de Ministros del Consejo de Europa emitió la Recomendación 95/4 sobre la protección de los datos de carácter personal en el ámbito de los servicios de telecomunicación, en especial con relación a los servicios telefónicos.

En 1995, el Consejo de Europa expidió la Recomendación 95/144/CE, relativa a los criterios comunes de evaluación de la seguridad en las tecnologías de la información, DO L 93 de 26.4.1995, pp. 27-28. En 1997, el Comité de Ministros del Consejo de Europa dictó la Recomendación 97/5, relativa a protección de datos médicos. Para 1999, el Grupo de Trabajo sobre la protección de las personas físicas aprobó la Recomendación 99/1, sobre el tratamiento invisible y automático de datos personales en internet efectuado por *software* y *hardware*.

Recopilando el contenido de varios de los dictámenes y recomendaciones citados, de las experiencias y principios desarrollados sobre todo en el ámbito jurisprudencial,[598] se expidieron dos Directivas:

a) Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la *protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*.[599] De la cual, debe

[598] Los Tribunales de Justicia alemanes son los primeros en reconocer el derecho a la protección de datos. Alemania: TRIBUNAL CONSTITUCIONAL FEDERAL, [Sentencia de 15 de diciembre de 1983, BJC 33, IV Jurisprudencia Constitucional Extrajera], 1984.

[599] DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación

recalcarse que en el artículo primero se señala que los Estados miembros garantizarán la protección de las libertades y de los derechos fundamentales de las personas físicas, haciendo expresa alusión al derecho a la intimidad.

b) Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre, relativa al *tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones*, que fue sustituida posteriormente por la Directiva 2002/58/CE, de 12 de julio, que establece un régimen específico para la protección de los datos de carácter personal en el ámbito de las telecomunicaciones y que ha sido transpuesta de forma parcial en el ordenamiento jurídico español, respecto de redes y servicios de telecomunicaciones electrónicas a través de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

La *Carta de los Derechos Fundamentales de la Unión Europea* 2000/C 364/01,[600] aprobada el 12 de enero de 2005, e incorporada al Tratado de Lisboa (Instrumento de Ratificación de 13 diciembre 2009), marca la independencia y autonomía que finalmente ha logrado el derecho a la autodeterminación informativa, ya que el artículo 7 se refiere al derecho a la intimidad como manifestación del respeto a la vida privada y familiar, del domicilio y de las comunicaciones; mientras que el artículo 8 se refiere a la protección de datos, entendido como un derecho que garantiza a toda persona la protección, control y acceso de sus datos de carácter personal:

> "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

El Tratado por el cual se establece una Constitución para Europa (que nunca llegó a entrar en vigor) reconocía a la autodeterminación informativa como un derecho fundamental

---

de estos datos (Diario Oficial n.° L 281, 23/11/1995, 0031-0050, s. f.), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML.

[600] DIARIO OFICIAL DE LAS COMUNIDADES EUROPEAS, *Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01)*, 18 de diciembre de 2000, http://www.europarl.europa.eu/charter/pdf/text_es.pdf.

distinto del derecho a la vida privada (artículo II-68),[601] e incluso recibía la calificación de elemento de la vida democrática en la Unión (artículo I-51).[602]

A partir de ese momento se han dictado otros cuerpos normativos de aplicación en el entorno europeo como:

El Reglamento 2001/45/CE, de 18 de diciembre de 2000, expedido por el Parlamento Europeo y del Consejo, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales por las Instituciones y los Organismos comunitarios y a la libre circulación de estos datos, DO L 8 de 12.1.2001. La Recomendación 2001/2, de 17 de mayo de 2001, sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea, elaborado por el grupo de trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Nota aparte merece el Tratado de Funcionamiento de la Unión Europea (TFUE), que en el artículo 16 (antiguo artículo 286 TCE) establece que toda persona tiene derecho a la protección de los datos de carácter personal y señala que el Parlamento Europeo y el Consejo establecerán normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por parte de instituciones, órganos y organismos de la Unión; así como por los Estados miembros y sobre la libre circulación de estos datos. Finalmente, se añade que el respeto de dichas normas estará sometido al control de autoridades independientes.

Cronológicamente se siguieron dictando los siguientes instrumentos: Reglamento (UE) n.º 611/2013, de 24 de junio de 2013, de la Comisión, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas. (DOUE 173, 26 de junio de 2013). Recomendación

[601] "Art. II-68. *Protección de datos de carácter personal* 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente". F. ALDECOA LUZÁRRAGA, ed. *Tratado por el que se establece una Constitución para Europa*, 2.ª ed. (Madrid, 2004), accedido 16 de junio del 2007, http://www.realinstitutoelcano.org/especiales/constitucioneuropea/nuevo/

[602] "Art. I-51. *Protección de datos de carácter personal* 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. La ley o ley marco europea establecerá las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes". F. ALDECOA LUZÁRRAGA, ed. *Tratado por el que se establece una Constitución para Europa*, 2.ª ed. (Madrid, 2004), accedido 16 de junio del 2007, http://www.realinstitutoelcano.org/especiales/constitucioneuropea/nuevo/

2014/724/UE, 10 de octubre de 2014, de la Comisión, relativa al modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente, Diario Oficial de la Unión Europea L n.º 300, 18 de octubre de 2014. La Directiva (UE) 2016/680, 27 de abril de 2016, del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por el que se deroga la Decisión Marco 2008/977/JAI del Consejo, DO L 119, 4 de mayo de 2016, y la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

Ahora bien, el desarrollo paulatino de la normativa europea citada, con altos niveles de especialidad, concreción de acuerdos mínimos puestos a prueba en los distintos Estados que conforman la Unión Europea, la creciente problemática del tratamiento de datos debido a la implementación de tecnologías emergentes, los avances en la jurisprudencia europea y los conflictos que propiciaron la caída de los acuerdos de puerto seguro posibilitaron que la Unión Europea dictara un Reglamento que deja de ser orientativo para volverse vinculante para sus Estados miembros y que apuesta por fortalecer el sistema de protección, así como viabilizar el flujo informacional.

El Reglamento (UE) 2016/679, 27 de abril de 2016, expedido por el Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, se denomina de manera general como Reglamento General de Protección de Datos o RGPD (por sus siglas en español o GDPR por su nombre en inglés *General Data Protection Regulation*) y ha tenido más de un año de *vacatio legis*, señalando para su puesta en vigencia, el 25 de mayo de 2018.

En ese sentido, la protección de datos personales con su contenido esencial (derechos, principios y autodeterminación informativa) se configura como derecho fundamental en los Tratados europeos, en las distintas jurisprudencias dictadas por los tribunales nacionales y comunitarios, en las normativas internas de cada país europeo y, finalmente, con el actual Reglamento Europeo de Protección de Datos Personales, de efecto vinculante y directo incluso sobre las normas internas para todo el territorio europeo. Todo lo cual refleja que en Europa se ha adoptado una dimensión objetiva de los derechos fundamentales, esto es la:

> [...] doble condición de objetos singulares regulados por normas constitucionales y de conjunto normativo constitucional que encarna una serie de caracteres en cuanto tal sistema. Dicho en otros términos, tal dimensión objetiva puede verse en la perspectiva individual de cada norma iusfundamental o en la perspectiva sistemática de la totalidad de normas iusfundamentales. Desde esta segunda óptica, de carácter sistemático, la jurisprudencia constitucional, primero en Alemania y después en el ámbito español, ha destacado la

> consideración de los derechos fundamentales como un sistema objetivo de valores que se encarnan en el ordenamiento jurídico como principios básico del orden constitucional. De esta forma, los derechos constitucionales en bloque se convierten en normas que fijan valores y fines vinculantes para el resto de las normas del ordenamiento y para los órganos productores y aplicadores de las mismas, trascendiendo así el mero sentido subjetivo de cada uno de ellos. Esto es lo que suele denominarse el efecto de irradiación de los derechos constitucionales, puesto que se proyectan hacia todo el ordenamiento e imponen a los poderes públicos la obligación de actuar positivamente en favor de su mayor eficacia.[603]

En resumen, nadie duda ahora que la protección de datos personales es un derecho fundamental, prueba de ello es la normativa constitucional y legal comunitaria y nacional existente, así como su aplicación por parte de autoridades competentes.

Ahora bien, sobre el contenido esencial del derecho se tratará en el título que corresponde, con la finalidad de identificar aquellos núcleos inamovibles del derecho y las innovaciones y cambios que son indispensables en el estado actual de la sociedad y de la técnica para garantizar la protección de datos personales de los ciudadanos y el movimiento de datos que permitan desarrollo económico.

5.3 Datos transfronterizos: Europa su relación con Estados Unidos

En la evolución de la concreción del derecho a la protección de datos personales como derecho fundamental, el desarrollo de un marco comunitario y su efectiva vigencia mediante las resoluciones dictadas por tribunales europeos, amerita acápite aparte la entrada en vigor de las Directivas 95/46/CE y Directiva 97/66/CE, relativas a la *protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y* al *tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones*, respectivamente. Constituyen los antecedentes visibles de este derecho y que, en su momento, se dictaron sin que la Unión Europea y Estados Unidos hubieran llegado a un acuerdo, pues no se pudieron conciliar los niveles de protección adecuados, sobre todo, respecto al sector privado americano y el uso secundario de datos recabados. Además, mientras Europa prohibía la transferencia de datos personales a otros países si estos no poseían un marco regulador aceptable en materia de privacidad, Estados Unidos sostenía que esta posición suponía una barrera para las transacciones por medio de internet. Sin embargo, "con el objeto de no impedir tajantemente los movimientos transfronterizos de datos personales, Europa y Estados Unidos celebraron el acuerdo conocido como *Safe Harbor* o «Acuerdo de Puerto Seguro»".[604]

---

[603] M. CARRASCO DURÁN y J. PÉREZ ROYO, *Curso de derecho constitucional* (Barcelona: Atelier, 2012).

[604] "La decisión sobre Puerto Seguro tiene varias características particulares: se trata de una decisión sectorial, es decir, declara 'adecuado' el nivel de protección a las empresas que aceptan someterse a sus reglas, no a un país entero. Además las empresas que deseen disfrutar de los beneficios que implica la adhesión a los principios de Puerto Seguro deben de cumplir con las siguientes condiciones mínimas: ser una compañía establecida en Estados Unidos, sujeta a la Comisión Federal de Comercio (FTC), o al Departamento de Transportes de los Estados Unidos (únicas entidades reconocidas hasta el momento por la Unión Europea)

A fin de regular las trasferencias internacionales de datos de los miembros de la Unión Europea con países carentes de un "nivel adecuado de protección", y para regular de alguna manera este tipo de operaciones, pese a no ser lo más adecuado, se dictaron los siguientes instrumentos relativos a la implementación de los llamados contratos tipo:

a) Dictamen 99/1, de 26 de enero de 1999, adoptado por el Grupo de trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales, relativo al nivel de protección de datos en Estados Unidos y a los debates entre la Comisión Europea y el Gobierno de Estados Unidos.

b) Dictamen 99/2, de 3 de mayo de 1999, adoptado por el Grupo de trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales, relativo a la idoneidad de los "Principios internacionales de puerto de seguro" que hizo públicos el Departamento estadounidense de Comercio el 19 de abril de 1999.

c) Decisión de 2001/497/CE, de 15 de junio, de la Comisión. *Protección de Datos. Cláusulas contractuales tipo para la transparencia de datos personales a un tercero país previstas en la Directiva 95/46/CE*, que se refiere a la transferencias de datos realizadas entre responsables del tratamiento, establecidos entre un Estado miembro de la UE y destinatarios fuera del territorio comunitario que actúen como encargados del tratamiento. Por lo tanto, la responsabilidad por incumplimiento y pago de la compensación recaerá de manera solidaria en los dos. El interesado tendrá, pues, derecho a emprender acciones y percibir una indemnización del importador de los datos o de ambos en caso de daños y perjuicios resultantes de cualquier acción incompatible con las obligaciones estipuladas en las cláusulas contractuales tipo.

d) Decisión 2002/16/CE, de 27 diciembre 2001, de la Comisión. *Protección de Datos. Cláusulas contractuales tipo para la transferencia de datos personales a los encargados de tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46 CE*. Por la cual, encargados de tratamiento establecidos en un país tercero, actuarán conforme a las instrucciones que reciba y a las obligaciones impuestas en las cláusulas. En caso de que el particular sufra un daño tendrá derecho a emprender acciones y, en su caso, recibir indemnización de parte del exportador de datos que sea responsable del tratamiento, excepto si hubiere

---

además de haber manifestado de forma inequívoca y pública su compromiso de cumplir las condiciones establecidas en este *Safe Harbor*. Los principios de Puerto Seguro son siete: notificación, opción, transferencia ulterior, seguridad, integridad de los datos, acceso y aplicación, mismos que se complementan por las Preguntas más Frecuentes (FACs) que precisan el alcance de éstos y pretenden aclarar algunas dudas respecto a su interpretación". X. PUENTE DE LA MORA, "Latinoamérica ante la tendencia europea y norteamericana en la regulación del flujo transfronterizo de datos personales", accedido 16 de junio del 2007, http://www.alfa-redi.org/rdi-articulo.shtml?x=7858

desaparecido, cesado de existir o fuere insolvente; en tales casos responderá el importador de datos subsidiariamente.

Pese a la firma del Acuerdo de puerto seguro, realizada el 26 de julio de 2000, su aplicación tuvo dificultades por la diversidad de las legislaciones aplicables en el espacio europeo, así como las instituciones responsables con distintos ámbitos y competencias.

Es para el año 2013 que el ciudadano austriaco Maximilliam Schrems presenta un reclamo al *Data Protection Commissioner* con sede en Irlanda, para que se prohibiera la transferencia de sus datos a Estados Unidos. Dicha petición fue negada por parte de dicha autoridad; sin embargo, al presentar un recurso ante la *High Court* de Irlanda, el alto tribunal declaró a Estados Unidos como un país que no tenía un nivel adecuado de protección por cuanto la legislación estadounidense no era compatible con la de la Unión Europea. Esta afirmación se realizaba sobre la base de que existía evidencia de que instituciones como el NSA o el FBI podían realizar operaciones de vigilancia e interceptación selectiva sin que exista pronunciamiento previo de viabilidad por parte de autoridad competente, postura contraria a la Constitución Irlandesa que establece el principio de proporcionalidad que obliga a que estas acciones deban estar debidamente motivadas y precautelen intereses colectivos.

Por cuanto las decisiones de la *High Court* no podían aplicarse extraterritorialmente, se suspendió el proceso y se planteó una acción ante el Tribunal de Justicia de la Unión Europea que, mediante sentencia de 6 de octubre de 2015, declaró la invalidez del Acuerdo de Puerto Seguro argumentando: a) falta de fiabilidad en la autocertificación, por falta de mecanismos que permitan constatar que se cumplen los principios establecidos; b) no existían garantías suficientes de que las empresas norteamericanas hayan implementado medidas de protección de datos; c) se permitía a las empresas acceder a datos personales directamente sin justificar y solicitar autorización previa de autoridad competente, por la mera sospecha de una afectación a la seguridad nacional o al interés público; d) se establecía mecanismos de solución de conflictos, pero no existían medidas de sanción para tratamientos inadecuados comprobados; e) no existía normativa específica que garantice protección en la transferencia de datos personales.

Sobre la base de esta argumentación se solicitó a Facebook que, hasta el 6 de enero de 2016, implementara medidas que garanticen un tratamiento adecuado. Esta situación propició negociaciones que llevaron a la firma de un nuevo acuerdo denominado Marco de Escudo de la Privacidad Unión Europea-Estados Unidos, acordado el 12 de julio de 2016, al que finalmente Facebook se adhirió con la finalidad de cumplir con la resolución judicial y continuar con el tratamiento de datos de ciudadanos europeos.

El Escudo de la privacidad refleja los requisitos establecidos por el Tribunal de Justicia de la Unión Europea de 2015, en la que declaraba inválido el marco de puerto seguro. Su contenido protege los derechos fundamentales de cualquier persona en la Unión Europea

cuyos datos personales se transfieran a los Estados Unidos, y para garantizar flujos de datos entre los dos continentes y otorgar seguridad jurídica a las empresas. Así se generaron normas más estrictas que buscan ser mejor aplicadas, especialmente aquellas salvaguardias respecto del acceso del Gobierno y también la implementación de un recurso más fácil para los particulares en caso de reclamaciones.[605]

El Escudo de la Privacidad UE-EE. UU.[606] se basa en los siguientes principios:

- Obligaciones de protección de datos (actualizaciones, revisiones, temporalidad en la retención y transferencias ulteriores a terceros) para las empresas que reciben datos personales de la Unión Europea.
- Limitaciones, salvaguardas, mecanismos de supervisión sobre el acceso del gobierno de Estados Unidos a los datos personales transferidos. Descartada la vigilancia masiva indiscriminada.
- Protección y reparación efectivas para las personas; en primer orden, reclamaciones resueltas por la propia empresa; o mecanismos de resolución alternativa de litigios gratuitos y en segundo nivel, posibilidad de dirigirse a sus autoridades nacionales de protección de datos. El recurso en el ámbito de la seguridad nacional para los ciudadanos de la UE será gestionado por un Defensor del pueblo independiente de los servicios de inteligencia de los Estados Unidos
- Revisión anual conjunta para monitorear la correcta aplicación del acuerdo.
- Recopilación en bloque de datos solo podrá utilizarse en condiciones específicas predeterminadas y tiene que ser lo más concreta y precisa posible.[607]

El Grupo de Trabajo del Artículo 29[608] ha realizado varios aportes relativos a internet de cosas, *cloud computing y Facebook*, puerto seguro, entre otros. Ahora será a CEPD a quien le tocará pronunciarse sobre la viabilidad o reformas a introducirse en el escudo de privacidad al ponerse en vigencia el Reglamento europeo que entró en vigor el 25 de mayo de 2018. Sobre todo porque, históricamente, Estados Unidos no ha sido declarado país con protección adecuada debido a su sistema de privacidad limitada, ya que el derecho a borrar solo puede utilizarse en casos especiales, mientras que el Reglamento es derecho de cada titular, por ejemplo.

---

[605] COMISIÓN EUROPEA, *La Comisión Europea pone en marcha el Escudo de la privacidad UE-EE.UU.: más protección para los flujos de datos transatlánticos*, accedido 25 de abril de 2018, http://europa.eu/rapid/press-release_IP-16-2461_es.htm.

[606] COMISIÓN EUROPEA, *Privacy Shield | Privacy Shield*, accedido 14 de mayo de 2018, https://www.privacyshield.gov/welcome.

[607] *Ibíd*.

[608] El Grupo de trabajo del artículo 29 es un grupo que responde de la Directiva 95/46/CE que fue lanzado en 1996 con la finalidad de dar otorgar directrices respecto del contenido de esta normativa y está compuesto por un representante de la autoridad de protección de datos de cada Estado miembro de la UE, el Supervisor Europeo de Protección de Datos y la Comisión Europea

Justice - Data Protection - Art.29 Data Protection Working Party, 20 de agosto de 2010, https://web.archive.org/web/20100820131123/http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

Más recientemente el CEPD ha adoptado el 22 de enero de 2019, el *EU - U.S. Privacy Shield - Second Annual Joint Review*[609], en el cual reconoce el avance que las autoridades estadounidense ha realizado para adaptar su actuación al marco normativo europeo, sobre todo desde la perceptiva comercial. Así como, aún persisten preocupaciones, en especial respecto de la recogida y el acceso masivo e indiscriminado a datos personales con fines de seguridad nacional, así como a la falta de designación de un Defensor del Pueblo permanente que tenga garantía e independencia.

5.4 Evolución de la normativa reguladora de la Protección de Datos de Carácter personal en España

La primera ley sobre protección de datos en España se dictó antes de la Directiva 95/46 del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y se denominó Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, de 29 de octubre de 1992, en cuya exposición de motivos había una alusión expresa al término *privacy*, que como vimos anteriormente, se configuró inicialmente en Estados Unidos como un:

> [...] poder de exclusión del conocimiento de los demás de la esfera personal, que es la idea que todavía hoy está extendida entre nosotros. Este concepto se ha ido ampliando hasta introducir una nueva acepción de la *privacy*. Se trata de la *privacy of autonomy o informational privacy*, con la que se intenta señalar el atentado a la persona perpetrado por la simple recogida y catalogación de informaciones, que se une al concepto tradicional de *privacy o disclosure*, en el que se engloban los atentados provocados por la difusión y revelación de noticias y datos personales cuyo conocimiento está limitado a un círculo restringido. En Estados Unidos de ninguna manera se afirma la existencia de un nuevo derecho fundamental de carácter informático, y mucho menos de un nuevo derecho de la personalidad. Allí la tutela frente a la informática deviene por tratarse de un atentado al derecho fundamental, el cual es la intimidad (*privacy*), pero adoptando un concepto de intimidad ampliado o extenso por su conexión a la libertad. Efectivamente en el ámbito de la informática, y sobre todo, frente al Estado, el sujeto que dispone del control de los datos que aquel maneja sobre él, puede desarrollar más ampliamente su libertad .[610]

Adicionalmente, el Tribunal Europeo de Derechos Humanos al determinar los contenidos de intimidad y vida privada sostuvo que es "posible distinguirlos al menos diferenciando diversos grados de intimidad dentro de la vida privada, que sería un concepto de cierta amplitud y de un alcance mayor del que tendría el concepto intimidad".[611]

---

[609] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *EU - U.S. Privacy Shield - Second Annual Joint Review*, 22 de enero de 2019, accedido el 174 de noviembre de 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf
[610] C. CONDE ORTIZ, *La protección de datos personales*, 24.
[611] C. RUIZ MIGUEL, *El derecho a la protección de la vida privada*, 35.

Todo lo cual contribuyó, aún más, a las contradicciones y posturas encontradas de la doctrina acerca de la existencia o no del derecho a la protección de datos, ya que la actual LOPD no tiene exposición de motivos y el término privacidad no aparece en ninguna parte de la ley.

Finalmente, la adecuada interpretación jurisprudencial de la Constitución dio como resultado el reconocimiento de un nuevo derecho, el de la autodeterminación informativa, cuyos principios rectores se desarrollaron en la Ley de Protección de Datos de Carácter Personal 15/1999, de 13 de diciembre (actualmente derogada), que es una transposición de la Directiva 95/46/CE, y que permite un adecuado, aunque perfectible, sistema de protección respecto del tratamiento de los datos personales en relación con el conjunto de libertades públicas y derechos fundamentales de las personas, con énfasis ya no solo en el derecho a la intimidad, sino en el derecho la autodeterminación informativa.

Los principios fundamentales para el tratamiento de datos a los que se hace referencia a lo largo de la ley son:

a) Consentimiento del afectado: libre, inequívoco, informado, revocable.
b) Calidad de datos: solo se podrán recoger y someter para su tratamiento, aquellos datos de carácter personal que sean adecuados, pertinentes y no excesivos en relación al ámbito de las finalidades determinadas, explícitas y legítimas (art. 4 LOPD).
c) Derecho de información en la recogida de datos de la existencia del fichero, de lo obligatorio o facultativo de sus respuestas, de las consecuencias de su obtención, de la posibilidad de ejercitar derechos de acceso, rectificación, cancelación y oposición, de la identidad del responsable.
d) Datos especialmente protegidos: los datos sensibles no pueden ser recabados sino por excepción, con el consentimiento previo expreso por escrito.

Como organismo que permite el cumplimiento de la normativa de protección de datos, y a fin de controlar la aplicación de la ley y verificar su adecuado ejercicio, se creó la Agencia Española de Protección de Datos, la cual, junto a otras tres autonómicas,[612] permite ir solucionando la creciente demanda.

Adicionalmente, España ha dictado otras dos normativas de carácter sectorial, la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y la Ley 32/2003, de 3 de noviembre, Ley General de Telecomunicaciones. Estas dos normas, además de regular aspectos sectoriales de la protección de datos personales en sus correspondientes ámbitos, atribuyen competencias en materia sancionadora a la Agencia Española de Protección de Datos.

[612] La de Madrid (Ley 13/1995, de 21 de abril, modificada por la Ley 8/2001, de 13 de julio, de Protección de Datos en la Comunidad de Madrid, y Decreto 67/2003, de 22 de mayo). La Catalana (Ley 5/2002, de 19 de abril, y Decreto 48/2003, de 20 de febrero); y La Vasca (Ley 2/2004, de 25 de febrero).

A causa de la necesidad de armonización entre las normas anteriormente citadas y en especial la necesidad de organizar en debida forma las competencias, atribuciones y potestades de la Agencia Española de Protección de Datos, se requirió un desarrollo reglamentario para lo cual se dictó el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, publicado en el Boletín Oficial Español, n.º 17, de 19/01/2008.[613]

Dicho Real Decreto, como reglamento de aplicación tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal; además otorga seguridad jurídica a las actuaciones de la Agencia de Protección de Datos Personales, puesto que concuerda los reales decretos 428/1993, de 26 de marzo, por el cual se aprobó el Estatuto de la Agencia de Protección de Datos. También está el Decreto 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, por el cual se aprobó el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, ya que establece criterios aplicables a los ficheros y tratamientos de datos personales no automatizados; y además, desarrolla procedimientos para el ejercicio de la potestad sancionadora por la Agencia en especial en el ámbito de sociedad de la información, del comercio electrónico y las telecomunicaciones.

Posteriormente, y como se verá en líneas posteriores, la normativa actualmente aplicable en España, luego de un proceso de elaboración iniciado en el 2012, es el Reglamento General de Protección de Datos (RGPD), publicado en el Diario Oficial de la Unión Europea en mayo de 2016, cuya entrada en vigencia se produjo el 25 de mayo de 2018, anotándose que debe ser de aplicación directa y que incluso se transpone a la normativa interna de cada país, en este caso de España. Sin embargo, pueden dictarse normativas para ayudar a su desarrollo, especialmente en aquellos casos en los que el citado reglamento realiza una remisión directa a una norma interna o en el que existen vacíos normativos que dificultan su concreción.

Por eso, España, al igual que los Estados miembros de la Unión Europea, a partir de la entrada en vigencia del RGPD, el 25 de mayo de 2018, inició un proceso de adaptación al RGPD. En este sentido, en el Boletín Oficial del Estado, nº. 183, del 30 de julio de 2018 se promulgó con n.º 70751, el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del derecho español a la normativa de la Unión Europea en materia de protección de datos (actualmente derogado).

En las consideraciones que motivan la promulgación de este Real Decreto constan las relativas a la propia remisión, que hace el RGPD a los Estados miembros de regular aspectos no tratados, por ejemplo, la regulación del estatuto de las autoridades de control. Asimismo, aquellas que carecen de remisión pero son necesarias completar para que la norma pueda ser aplicable, por ejemplo los plazos de prescripción de las infracciones. Sin

[613] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, 21 de diciembre de 2007, https://www.boe.es/buscar/act.php?id=BOE-A-2008-979.

embargo, la norma solo alude a aquellas temáticas que pueden ser tratadas a nivel de un Real Decreto, por no estar excluidas del ámbito del legislador de urgencia —artículo 86 de la Constitución española— y son indispensables y urgentes para la entrada en vigencia del RGPD. El Real Decreto-Ley contiene tres capítulos, catorce artículos, dos disposiciones adicionales, dos transitorias, una derogatoria y una final.

El capítulo I regula el personal competente para el ejercicio de los poderes de investigación previstos en el artículo 58.1 del RGPD y el régimen aplicable al personal de las autoridades de supervisión de otros Estados miembros que participen en actuaciones conjuntas de investigación.

El capítulo II desarrolla aquellos elementos necesarios para el funcionamiento del nuevo régimen sancionador establecido por el RGPD.

El capítulo III contiene los procedimientos de atención para los supuestos de vulneración del RGPD que sean reclamados ante las autoridades de control local y aquellas que pudieran ser parte de un mecanismo de coherencia.

La disposición adicional primera designa como representante de España en el Comité Europeo a la Agencia Española de Protección de Datos.

La disposición adicional segunda contiene previsiones en lo relativo a la publicidad de las resoluciones de la Agencia Española de Protección de Datos, con el fin de garantizar la transparencia de su actuación, ante el nuevo marco procedimental configurado por el Reglamento General de Protección de Datos.

Finalmente, se dicta la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[614], en adelante LOPDGDD. Esta normativa en la Disposición derogatoria única. Deroga la hasta entonces vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sin perjuicio de lo señalado en la disposición adicional decimocuarta[615] y en la disposición transitoria

[614] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, BOE.es, accedido 13 de noviembre de 2018, file:///C:/Users/Lorena/Desktop/Ley%20Protecci%C3%B3n%20datos%20y%20derechos%20digitales%20Espa%C3%B1a.pdf

[615] La Disposición adicional decimocuarta se refiere a las normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE, que se refiere a las excepciones y limitaciones en el ejercicio de los derechos que hubiesen entrado en vigor con anterioridad a la fecha de aplicación del reglamento europeo y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Por la cual, estas excepciones seguirán vigentes, a menos que sean expresamente modificadas, sustituidas o derogadas, si bien son referidos a los derechos tal y como se regulan en el Reglamento (UE) 2016/679 y en esta ley orgánica. Es decir, respecto de ficheros de: a) Fuerzas y Cuerpos de Seguridad para fines administrativos, policiales para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, absolutamente necesarias para una investigación concreta; y b) Hacienda Pública, En estos casos, los responsables podrán no entregar información de transparencia o seguir recopilando información a través de formularios, o denegar el acceso, la rectificación o cancelación en

cuarta[616]; el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos y aquellas disposiciones de igual o inferior rango que contradigan, opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y esta nueva ley orgánica.

La citada LOPDGDD se encuentra en vigor en España desde el 7 de diciembre de 2018, y establece una serie de precisiones respecto de aquellos temas que, el Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[617] (en adelante, RGPD), deja a cada Estado para pronunciarse. Y es que, cada país miembro de la Unión, para garantizar seguridad jurídica, deben adecuar su normativa interna de manera que la desarrolle y permita su eficaz aplicación o, de ser el caso, elimine contradicciones o incompatibilidades.

Lo más destacable de la LOPDGDD, es que al tenor de lo dispuesto en el artículo 18.4 de la Constitución española, que señala: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", se reconocen a nivel legal nuevos derechos, y en este sentido, representa la normativa más avanzada en el mundo. Estos derechos digitales constan en Título X denominado: Garantía de los derechos digitales desde el artículo 79 al 96 de la citada normativa y son los que se enlistan a continuación: derecho a la neutralidad de internet, derecho de acceso universal a internet, derecho a la seguridad digital, derecho a la educación digital, protección de los menores en internet, derecho de rectificación en internet, derecho a la actualización de informaciones en medios de comunicación digitales, derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, derecho a la desconexión digital en el ámbito laboral, derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral, derechos digitales en la negociación colectiva, protección de datos de los menores en internet, derecho al olvido en búsquedas de internet, derecho al olvido en servicios de redes sociales y servicios equivalentes, derecho de portabilidad en servicios de redes sociales y servicios equivalentes y derecho al testamento digital.

Ahora bien, cuando se realice el análisis del contenido esencial del derecho a la protección de datos personales en Europa además de revisar el contenido del RGPD se analizará la

función de los peligros que pudieran derivarse para la defensa del Estado, la seguridad pública, la protección de los derechos y libertades de terceros, las funciones de control o verificación de las administraciones públicas, incluidas las obligaciones tributarias y las actuaciones inspectoras; así como las investigaciones penales o administrativas.

[616] Disposición adicional cuarta, que se refiere al procedimiento en relación con las competencias atribuidas por otras leyes a la Agencia Española de Protección de Datos.

[617] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) Documento DOUE-L-2016-80807, BOE.es, accedido 16 de mayo de 2018, https://www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80807.

adaptación que la LOPDGDD española ha realizado, incluidos aquellos derechos digitales que constan desarrollados en estos textos normativos y que tiene relación directa con la protección de datos personales, de tal forma que, aun siendo parte de este derecho, el legislador español ha considerado necesario darle autonomía e identidad propia.

5.5 Estado actual de la situación de la protección de datos personales en el contexto europeo

Mediante el análisis cronológico de los instrumentos citados se vislumbra el progreso que ha tenido en Europa el derecho a la libertad informática. Y puede decirse que la normativa europea tiene un carácter especialmente preventivo.

Es fruto de un proceso de formación de conciencia sobre el derecho a la protección de datos, ya que inicialmente fue concebida como una manifestación negativa del derecho a la intimidad, es decir, un derecho de defensa frente a cualquier agresión a la esfera privada de una persona. En este sentido, Concepción Conde señala que el derecho a la protección de datos personales se diferencia de la intimidad porque el primero tiene una función de exclusión de ciertos datos de una persona al conocimiento ajeno, mientras que el segundo permite a la persona disponer de su acervo de datos. Por lo que, el contenido de este derecho es más amplio debido a que no interesa si la información forma parte de un dato personal íntimo o privado, sino de una generalidad de datos de carácter personal.[618]

A causa de la versatilidad de los tratamientos tecnológicos que se pueden realizar con los datos de una persona, en los que incluso datos aparentemente inocuos pueden revelar perfiles de la personalidad, que incluyan posturas ideologías, estados económicos, sociales, culturales e incluso emocionales o cualquier otra información que puede convertirse en una amenaza para el desarrollo de la libre personalidad del individuo,[619] obligan a los Estados a otorgar un derecho que no puede agotarse en la protección de los datos íntimos o privados, sino que debe tutelar cualquier tipo de dato; porque la utilización de estos no solo afecta a la intimidad, sino a otros derechos fundamentales como la salud, el trabajo, la vivienda, etc.

El derecho a la autodeterminación informativa se configura como un derecho fundamental independiente y autónomo por el cual todas las personas tienen derecho a controlar sus datos de carácter personal; es decir, decidir cuáles datos, en qué condiciones y con qué finalidad desea facilitarlos.

El *habeas data* o simplemente los derechos de acceso, rectificación, cancelación y oposición propios del titular son parte del contenido esencial del derecho, tal como se ha señalado:

---

[618] Concepción CONDE ORTIZ, *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad* (Madrid: Dykinson, 2005), 46.
[619] CONDE ORTIZ, 46.

> [...] el derecho al control sobre los datos personales almacenados y tratados en archivos informáticos se conoce con el nombre de libertad informática y tiene su principal garantía en el hábeas data, es decir la facultad de las personas de conocer y controlar las informaciones que les conciernen procesadas en bancos informatizados [...] se condensa en la noción de hábeas data, que significa tener o controlar los datos personales sometidos a almacenamiento y tratamiento informatizado. Este control implica, al menos, las siguientes facultades: tener conocimiento sobre la existencia y caracteres de los ficheros; disponer del derecho de acceso a los ficheros; ejercer los derechos rectificación y cancelación de datos inexactos o ya superados, con algunas excepciones por razones de seguridad pública (defensa del Estado, derechos y libertades de terceros o necesidades de investigaciones criminales en curso). Estos derechos se reconocen en el artículo 14 de la Ley orgánica 15/1999 (desarrollada por el Real decreto 1720/2007) [de España]. Esta regulación determina el derecho de toda persona a conocer la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. Estos datos deberán obtenerse recabando la información correspondiente del Registro General de Protección de Datos, siendo la consulta pública y gratuita. En cuanto a la concreción del derecho de hábeas data, la Ley establece con claridad el derecho dela persona interesada a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismo. Por otra parte, se recoge el derecho de rectificación y cancelación que correrá a cargo del responsable del tratamiento y deberá efectuarlo, en el plazo de diez días desde la solicitud, cuando los datos de carácter personal hayan sido tratados al margen de las previsiones de la Ley y, en particular, cuanto tales datos resulten inexactos o incompletos.[620]

En el mismo sentido, María Mercedes Serrano Pérez señala que los derechos propios de la protección de datos: "Constituye manifestaciones concretas de poderes que puede articular la propia persona para la defensa de sus intereses y al mismo tiempo, la contrapartida que equilibra el poderoso potencial que representa la informática".[621] Y estos poderes de decisión se manifiestan "a través de los derechos de acceso, rectificación, cancelación y oposición, también conocidos como derechos ARCO, podemos saber qué información personal se está tratando por un responsable, de quien o de dónde se obtuvieron los datos y a quién se los ha cedido. Modificar o rectificar errores, cancelar datos que no se deberían estar tratando u oponernos a tratamientos de datos personales realizados sin nuestro consentimiento".[622]

Otro de los elementos que forma parte del contenido esencial del derecho a la protección de datos personales corresponde a la entidad que supervisa su comprensión, regulación y

[620] M. APARICIO PÉREZ y M. BARCELÓ I SERRAMALERA, eds., *Curso de derecho constitucional* (Barcelona: Atelier, 2012), 712-3.
[621] M. SERRANO PÉREZ, *El derecho fundamental a la protección de datos: derecho español y comparado*, Estudios de protección de datos (Madrid: Civitas, 2003), 343.
[622] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, accedido 14 de mayo de 2018, https://www.agpd.es/portalwebAGPD/index-ides-idphp.php.

cumplimiento, puesto que la norma sin autoridad que vele por su vigencia resulta inútil. En este sentido se prevé que:

> [...] la ley exige la creación de una agencia de protección de Datos como ente de derecho público, con personalidad jurídica propia y plana capacidad pública y privada, que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones. Igualmente, se insta por la propia Ley a la creación de agencias autonómicas, responsables de los datos por ellas gestionados y por entes locales. Entre las funciones que deben cubrir dicho ente se encuentran: velar por el cumplimiento de la legislación sobre protección de datos, controlar su aplicación y los derechos de las personas que puedan estar afectadas, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos. Igualmente, es responsable de emitir las autorizaciones preceptivas, así como de requisita a los responsables y los encargos de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para adecuación del tratamiento de las disposiciones de la citada Ley y, en su caso, ejercer la potestad sancionadora y ordenar la cesación de los tratamientos y a cancelación de los ficheros, cuando no se ajuste a sus disposiciones.[623]

Finalmente, de la mano de uno de los padres de la protección de datos personales en España, el filósofo Antonio Enrique Pérez Luño, se puede identificar la evolución tecnológica y normativa de este derecho:

> [...] desde las leyes de la primera generación, basadas en la autorización previa de los bancos de datos en un etapa en la que los equipos informáticos eran escasos, voluminosos y fácilmente localizables; a las leyes de la segunda generación, cuyo principal objetivo fue la garantía de los datos sensibles, por su inmediata incidencia en la privacidad o su riesgo para prácticas discriminatorias; y, en la actualidad, a las de la tercera generación, que se han hecho cargo de la revolución microinformática con la consiguiente difusión capilar de los bancos de datos. Ello ha hecho prácticamente inviable el control previo de los equipos informáticos, sobre el que operaron las normas de la primera generación; al tiempo que la tutela de las informaciones ya no puede quedar circunscrita al factor estático de su calidad, según el criterio predominante en la segunda generación de leyes de protección de datos, sino que debe hacerse extensiva a la dinámica de uso o funcionalidad [...] no se limita a su tutela en cuanto meros depósitos de informaciones, sino también y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados. Así parece desprenderse de la definición de tratamiento de datos, que viene entendida como operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas interconexiones y transferencias [...] de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.[624]

[623] PÉREZ Y BARCELÓ I SERRAMALERA, *Curso de derecho constitucional*, 714.
[624] A. PÉREZ LUÑO, *Derechos humanos, estado de derecho y constitución*, 7.ª ed. (Madrid: Tecnos, 2001), 372-3.

En suma, se está ante la presencia de un derecho cuya existencia es relativamente reciente, menos de 40 años (38 años, si se considera al Convenio 108/81, de 28 de enero de 1981, como la primera normativa que lo reconoce oficialmente) si se la compara con otros de larga data. Que sigue configurándose paulatinamente, en la medida que la tecnología, que es su inminente moduladora, avanza y propone nuevas formas de manipulación, procesamiento, tratamiento, utilización, cesión de los datos personales, etc.

Prueba de ello, son los actuales reclamos suscitados por el Senado americano al creador de la red más grande del mundo. Debido a una filtración de seguridad de la red social se permitió la entrega de datos, 87 millones (2,7 millones de ciudadanos europeos) de usuarios de *Facebook*, a la Compañía *Cambridge Analytica*, sin que ellos lo supieran.

> Este "botín informativo sirvió al equipo de Donald Trump para segmentar a los votantes en su carrera a la Casa Blanca y también fue explotado por las plataformas partidarias del Brexit en Reino Unido. Además, según la propia empresa, los perfiles de la mayoría de su ingente comunidad de miembros —2.200 millones— eran vulnerables a ataques de este tipo. [...] Las elecciones presidenciales [americanas] de noviembre de 2016 pusieron sobre la mesa el uso perverso de las redes sociales para difundir informaciones falsas, fomentar la división y —en el caso de la trama rusa— intentar favorecer la victoria electoral de Trump. El pasado octubre Facebook admitió que la propaganda rusa había alcanzado hasta a 126 millones de usuarios entre enero de 2015 y agosto de 2017.[625]

Por ello, Giovanni Buttarelli, Supervisor Europeo de Protección de Datos dicta en Bruselas, el 19 de marzo de 2018, emite el Dictamen 2018/C 233/06 sobre manipulación en línea y los datos personales, en el cual se dimensiona lo siguiente:

> El problema del uso de la información y los datos personales para manipular a los ciudadanos y la política va mucho más allá, sin duda, del derecho a la protección de datos. Un entorno en línea personalizado y microsegmentado crea «burbujas de filtro» que hacen que los ciudadanos estén expuestos a información que es «más de lo mismo» y encuentren menos opiniones, lo cual lleva a una mayor polarización política e ideológica (7). Aumenta la omnipresencia y la persuasión de historias falsas y conspiraciones (8). Los estudios apuntan a que la manipulación de los canales de noticias o de los resultados de las búsquedas de los ciudadanos podrían influir en su decisión de voto (9).[626]

Si bien, en las fases de evolución tecnológica y normativa del derecho a la protección de datos personales, Perez Luño señaló que nos encontramos en una tercera generación de leyes que intenta evitar el abuso en el uso y la finalidad del tratamiento de los datos personales, ahora nos encontramos en una nueva fase en la que, se debe precautelarse la voluntad humana en todas sus dimensiones: comercial, contractual, libertad, pensamiento,

[625] A. MARS, "Zuckerberg pide perdón en el Senado y advierte de la amenaza de Rusia", *El País*, 11 de abril de 2018, sec. Internacional, https://elpais.com/internacional/2018/04/10/actualidad/1523380980_341139.html.
[626] G. BUTTARELLI, *Dictamen 2018/C 233/06 sobre la manipulación en línea y los datos personales*, Supervisor Europeo de Protección de Datos, 19 de marzo de 2018, accedido el 11 de noviembre de 2019, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_summary_es.pdf

expresión, desarrollo de su propia personalidad, pero sobre todo, a decidir sobre el ejercicio de sus derechos, entre ellos, el derecho al voto y a elegir a sus representantes, sin injerencias abusivas, arbitrarias o manipuladoras.

Lamentablemente, las Tics pueden ser usadas como mecanismos de control social. Ya que se puede modelar la conducta humana de tal forma que, ya no solo se persuada, a través de técnicas de mercadeo, de comunicación estratégica, de psicología social, *neurohacking*[627], entre otras, sino que se llegue a la manipulación. Es decir, se induzca a un comportamiento o emoción que solo beneficia o favorece a quien manipula. El manipulado no puede tomar previsiones, no ha realizado un análisis crítico y ha sucumbido su voluntad respondiendo a la manipulación. Entonces, se puede concluir que el manipulador tiene como simple objetivo el control de la voluntad del individuo.

En este sentido, la trasgresión de los derechos humanos en internet se torna evidente y por ello, "la solución radica en hacer cumplir las normas ya existentes, en particular el RGPD, rigurosa y conjuntamente con otras normas aplicables a las elecciones y al pluralismo en los medios de comunicación" [628].

Finalmente, el Informe sobre la economía digital 2019: creación y captura de valor: repercusiones para los países en desarrollo dictada por la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, UNCTAD determina que:

> Ha surgido una "cadena de valor de los datos" completamente nueva que incluye a las empresas que promueven la recopilación de datos; la elaboración de conocimiento a partir de los datos; y el almacenamiento, análisis y modelización de esos datos. La creación de valor surge una vez que los datos se transforman en inteligencia digital y se monetizan a través de su utilización comercial. El control de los datos es importante desde el punto de vista estratégico para poder transformarlos en inteligencia digital (…) Las empresas centradas en plataformas gozan de una gran ventaja en la economía basada en los datos. Al operar al mismo tiempo como intermediarios e infraestructura, están en condiciones de registrar y extraer todos los datos relacionados con las acciones de los usuarios de la plataforma y de sus interacciones en línea.[629]

En este sentido, la posibilidad de controlar los datos puede significar la de modelar economías y sociedades enteras, por ello la necesidad de conjugar los derechos del consumidor, su capacidad de elección evitando la clientela cautiva, por ejemplo; la privacidad; y, el derecho la protección de los datos personales con normativas sobre control de poder de mercados que permita hacer frente a estas grandes plataformas, a estos

---

[627] P. KELLMEYER, *Big Brain Data: On the Responsible Use of Brain Data from Clinical and Consumer-Directed Neurotechnological Devices; (Springer, 2018), accedido el 11 de noviembre de 2019* https://doi.org/10.1007/s12152-018-9371-x.

[628] Ibíd.

[629] ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Informe sobre la economía digital 2019: creación y captura de valor: repercusiones para los países en desarrollo,* 04 de septiembre de 2019, accedido el 11 de noviembre de 2019.

"operadores digitales dominantes, por ejemplo, definiendo cuidadosamente el mercado de referencia, evaluando el posible abuso de poder en el mercado y actualizando los instrumentos de control de las fusiones de empresas". [630]

Pero además, se debe trabajar no solo en lograr acceso a internet y tics; desarrollar la confianza digital de los consumidores y en fortalecimiento de la ciberseguridad; sino y de manera especial, en el desarrollo de capacidades digitales que permitan la "generación de valor añadido en las cadenas de valor de los datos" [631] y también en la de "refinar" [632] esos datos, principalmente por parte de emprendedores, profesionales, Pymes y grandes empresas de aquellos países en situación de desventaja, por ser meros proveedores de datos brutos y consumidores de inteligencia de datos. Todo lo cual, permitirá una distribución más justa de la riqueza digital, es decir de los beneficios derivados de los datos y la inteligencia digital; así como, estar en "mejores condiciones para hacer frente a los riesgos y desafíos asociados a la expansión de los datos digitales" [633].

> Y este postulado junto con políticas públicas de apoyo a la innovación y al desarrollo de capacidades digitales apunta corregir los desequilibrios mundiales y lograr una adecuada repartición de "beneficios de la economía digital". Toda vez que, la riqueza digital, entendida como las ganancias producidas por la expansión de la digitalización, de las conexiones de Internet y las compras en línea" está concentrada en manos de unas cuantas plataformas implantadas en los Estados Unidos y en China", que ha generado desigualdades que, sin acciones inmediatas y claras, seguirá profundizado la brecha entre "países infraconectados y países hiperdigitalizados" y aquellos como África y América Latina, que se han limitado a ser usuarios y consumidores y no han logrado ser "productores, exportadores e innovadores, para crear y capturar más valor en su camino hacia una prosperidad inclusiva". [634]

En este escenario, el derecho a la protección de datos personales se torna el centro, la base de la defensa de los derechos humanos en línea. Por ello, su núcleo básico, su contenido esencial, debido a la constante y vertiginosa evolución de la tecnología, debe ser adaptable y estar en continua complementariedad e integralidad con otros derechos para cumplir con su objetivo primordial: salvaguardar la dignidad de las personas, ya que lo virtual afecta o causa daño en la realidad no solo a la persona individualmente considerada, sino a toda la sociedad, en todos los ámbitos político, social y cultural; sobre todo en la prosperidad y desarrollo económico e incluso en los valores más básicos de formación social como es la democracia.

---

[630] Ibíd.
[631] Ibíd.
[632] Ibíd.
[633] Ibíd.
[634] ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Informe sobre la economía digital 2019: creación y captura de valor: repercusiones para los países en desarrollo,* 04 de septiembre de 2019, accedido el 11 de noviembre de 2019.

6. Protección de datos en la normativa europea, análisis del Reglamento europeo de protección de datos personales

Conforme consta en la exposición de motivos del RGPD las situaciones reales que motivaban la necesidad de promulgar una normativa vinculante para la comunidad europea convergen en la fragmentada aplicación de la Directiva 95/46/CE.[635] Si bien dicha Directiva, estableció una normativa común en la Unión Europea, para la protección del tratamiento de datos personales y su libre circulación, su aplicación durante estos más de 10 años ha sido heterogénea, pues su contenido ha sido legislado en cada país de la unión, con sus propias precisiones o especificidades; las cortes nacionales han desarrollado sus propias jurisprudencias; y, se han creado y fortalecido institucionalidades dependiendo de las necesidades y situaciones de cada estado.

Y es que las Directivas, por tratarse de normativas de naturaleza no imperativa, facultan a cada Estado a adoptarlas en su legislación interna, estableciéndose los diferentes niveles de protección antes descritos y divergencias en la ejecución y aplicación de la normativa comunitaria y nacional mediante los distintos órganos competentes.

El considerando (9) del RGPD menciona que esta falta de homogeneidad provocaba inseguridad jurídica, así como la percepción generalizada entre la opinión pública de que no existen riesgos importantes para la protección de las personas físicas en sus actividades en línea, o en el tratamiento de sus datos personales, así como una restricción real en la circulación de los datos de carácter personal en la comunidad, que pueden constituir en obstáculo al ejercicio de las actividades económicas a nivel de la Unión, o que permitan falsear la competencia o impedir que las autoridades cumplan sus funciones.[636]

Asimismo, en el contexto mundial, los riesgos en el uso de datos personales se han intensificado debido al incremento de la interoperabilidad mundial y de los flujos transfronterizos de datos; del uso de tecnologías invasivas de la privacidad como la vigilancia, el monitoreo las interceptaciones y el internet de las cosas; del almacenamiento y tratamiento masivo de datos personales, incluidos datos biométricos, metadados y fragmentos de datos; de la elaboración de perfiles de personalidad: predictivos, de confiabilidad y de comportamiento, entre otros; de la implementación de valoraciones o decisiones automatizadas; de la utilización de algoritmos de tratamiento inaccesibles para revisión de posibles sesgos discriminatorios; el aprendizaje automático o la inteligencia artificial, en sus distintas variantes, incluido el *neurohacking*; así como, de visualización de contenidos microdirigidos que dejan poco lugar para el consentimiento o el control que el

[635] DIRECTIVA 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[636] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) Documento DOUE-L-2016-80807.

individuo pueda dar o hacer respecto de su información"[637] y de los efectos transnacionales de los daños producidos por usos indebidos de datos personales.

La realidad jurídica, la dificultad de la aplicación práctica del sistema de protección, unida al vertiginoso desarrollo tecnológico, la creatividad y la innovación no solo para la ciencia sino para la implementación de nuevos servicios y modelos de negocio, las nuevas respuestas estatales a las realidad de la era digital e incluso la propia conducta humana en línea, han marcado un reto para la normativa. Y es que, tradicionalmente, el derecho, que siempre va por detrás de las problemáticas sociales, pues los regula cuando estos ya han ocurrido. En el caso de la ciencia y la tecnología asociada con los datos personales esta tardía forma tradicional de respuesta resulta ineficaz al extremo. Por ello es que, se requiere de normativas homogéneas, de aplicación vinculante general, orientativas para otras regiones del planeta, amparada en normativa internacional de derechos humanos y redactada a manera de principios, derechos y obligaciones como un marco referencial de actuaciones lícitas, legítimas, respetuosas de la dignidad humana, que pudieran hacer frente a esta problemática compleja.

Si bien, los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, es indispensable una norma vinculante de aplicación y ejecución irrestricta en el mayor número de países, de ahí que la Unión Europa es el mejor ejemplo a seguir, al haber dictado el Reglamento General de Protección de Datos, RGPD.

Su aplicación es obligatoria, directa e incluso por encima de leyes nacionales. Además, propicia la derogatoria de las normativas internas pertinentes y la adaptación de otras. Busca un sistema de protección práctico, jurídico y técnico coherente y homogéneo que "establezca el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros", considerando (13).[638] Es decir, una actuación integral que garantice "un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión", conforme consta en el considerando (10) del citado reglamento.[639]

La Comisión Europea trató la primera propuesta de Reglamento General de Protección de Datos en enero de 2012. Para marzo de 2014, el Parlamento Europeo votó a favor de las nuevas leyes de protección de datos. En junio de 2015 los ministros de los Estados miembros, el Consejo de Justicia y Asuntos de Interior de la Unión Europea acordaron un enfoque general del reglamento. En mayo de 2016, el Reglamento General de Protección de

[637] V. MILANÉS, *El sistema de protección de datos personales en América Latina: Oportunidades y desafíos para los derechos humanos*, volumen 1, (Asociación por los Derechos Civiles (ADC): diciembre 2016) accedido el 11 de noviembre de 2018, https://adcdigital.org.ar/wp-content/uploads/2017/06/Sistema-proteccion-datos-personales-LatAm.pdf
[638] Reglamento (UE) 2016/679.
[639] Ibíd.

Datos fue publicado en el Diario Oficial de la Unión Europea. Finalmente, entró en vigencia, el 25 de mayo de 2018, por lo que todos los Estados miembros deben transponerlo en su legislación nacional.

La aprobación del RGPD determina la derogatoria de la Directiva 95/46/CE.[640] Tampoco seguirá vigente la normativa nacional de cada país miembro de la Unión Europea, sino que el reglamento deberá aplicarse directamente de forma vinculante por todos los Estados. Incluso el "Reglamento (CE) N.O. 45/2001 del Parlamento Europeo y del Consejo se aplica al tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión; y, otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal deben adaptarse a los principios y normas establecidos en el Reglamento y aplicarse a la luz del mismo. A fin de establecer un marco sólido y coherente en materia de protección de datos en la Unión, una vez adoptado el Reglamento deben introducirse las adaptaciones necesarias del Reglamento (CE) N.O. 45/2001, con el fin de que pueda aplicarse al mismo tiempo que el Reglamento".[641]

Según el considerando (171) del RGPD todo tratamiento iniciado antes de la vigencia del reglamento debe ajustarse en el plazo de dos años a partir de la fecha de su entrada en vigor. Respecto del consentimiento, si este fue obtenido se ajusta a las condiciones del Reglamento, no siendo necesario recabarlo nuevamente, pero si en contrario sentido.

Por tanto, es importante destacar que el objeto del actual RGDP es completo; en otras palabras, aborda desde varias perspectivas el tratamiento de datos personales, lo que lo convierte en un cuerpo normativo con una visión integral que intenta encontrar el justo balance entre la persona y sus derechos, así como el desarrollo económico. Todo ello de la mano del uso y disfrute positivo de los avances tecnológicos.

Conforme los considerandos preliminares del RGPD, esta normativa desarrolla el siguiente contenido:

a) *Evolución tecnológica y globalización:* Los avances vertiginosos en ciencia y tecnología, la globalización como fenómeno complejo, la hiperconexión a la que están sometidas las personas, la sobreexposición de las personas físicas reflejan el aumento de interacciones a escala mundial. Los voluminosos datos personales y los actuales métodos para analítica de datos han transformado la política, la economía, la educación, la cultura, la vida social. Este entorno plantea nuevos retos para la protección de los datos personales, pues las formas de protección tradicionales deben ser revaluadas especialmente bajo la mirada de tecnologías emergentes que ponen a prueba los sistemas de regulación y protección, pues debe garantizarse un

[640] RGPD 2016/679. Capítulo XI, Disposiciones finales, artículo 94, Derogación de la Directiva 95/46/CE: **"**1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018. 2. Toda referencia a la Directiva derogada se entenderá hecha al Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el Reglamento".
[641] RGPD 2016/679, considerando número (17).

libre flujo de información que favorezca a la economía, pero al mismo tiempo mantenga un elevado nivel de protección de los datos personales.

b) *Derecho a la protección de datos personales:* El reconocimiento de la protección de datos personales como derecho fundamental, de conformidad con lo señalado en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea[642] y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE).[643]

c) *Respeto a las libertades individuales y derechos fundamentales:* Es decir, mediante esta norma se protege a la persona en sus relaciones dentro de la denominada sociedad red, esto es a la vida privada y familiar, domicilio, comunicaciones, protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, derecho a la tutela judicial efectiva y a un juicio justo, a la diversidad cultural, religiosa y lingüística, entre otras que han tenido que redefinirse y modificar su alcance en la era digital.

d) *Derechos y obligaciones:* La protección de los datos personales se refuerza por medio de la clara determinación de los derechos de los individuos y de las obligaciones de quienes tratan y determinan el tratamiento de sus datos; así mismo, el fortalecimiento de las entidades estatales de control que se nutran de "poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes", al tenor de lo señalado en el considerando (11).[644]

e) *Principio de proporcionalidad:* El derecho a la protección de los datos personales no es absoluto, debido a que debe mirarse la función social que cumple en desarrollo tecnológico y económico de los Estados. Por eso, se deberá aplicar el principio de proporcionalidad de manera que se pueda mantener un equilibrio con otros derechos fundamentales como el acceso de tecnología, a bienes y servicios privados y públicos de calidad, al desarrollo económico, social y cultural, entre otros.

f) *Necesidad de armonización:* Si bien, la necesidad de armonizar la protección de los derechos y las libertades individuales respecto del tratamiento de datos de carácter personal y al mismo tiempo garantizar la libre circulación de estos datos entre los Estados miembros, se desarrolló en la derogada Directiva 95/46/CE del Parlamento Europeo y del Consejo, su abordaje se profundiza en el RGPD debido a los avances de la ciencia y la tecnología. El establecer un nivel uniforme, coherente y elevado de protección mediante un marco normativo equivalente en todos los Estados miembros es una garantía real de los derechos y las obligaciones de las personas en la era digital. Además, la uniformidad elimina los obstáculos a la circulación de

[642] DIARIO OFICIAL DE LAS COMUNIDADES EUROPEAS, *Carta de los Derechos Fundamentales de la Unión Europea* (2000/C 364/01).

[643] ESTADOS MIEMBROS DE LA UNIÓN EUROPEA, *Tratado de Funcionamiento de la Unión Europea, versión consolidada* (C 83/50. Diario Oficial de la Unión Europea 30.3.2010, s. f.), https://www.boe.es/doue/2010/083/Z00047-00199.pdf.

[644] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) Documento DOUE-L-2016-80807.

datos personales dentro de la Unión Europea y esto además de mejorar el libre flujo de la información favorece el desarrollo económico. Asimismo, los Estados miembros están facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del Reglamento (10).[645] En el mismo sentido el artículo 98 del RGPD señala en las disposiciones finales que la Comisión de ser procedente podrá "presentar propuestas legislativas para modificar otros actos jurídicos de la Unión en materia de protección de datos personales, a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento. Se tratará en particular de las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento por parte de las instituciones, órganos, y organismos de la Unión y a la libre circulación de tales datos", en especial las relativas al Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000. Pero esta armonización no solo debe ser vista desde la perspectiva de generar un marco técnico, tecnológico y regulatorio que favorezca la interoperabilidad y el libre flujo transfronterizo datos, sino que propenda al desarrollo de capacidades institucionales, de entes públicos y privados que logren obtener valor del dato y su respectiva inteligencia[646] y por ende promuevan una mejora sustancial en la economía digital de los países europeos, pero no solo de estos, sino que estas mismas estrategias se efectivicen para Latinoamérica.[647]

g) *Marco sólido y coherente:* Es decir, promover la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas. La seguridad jurídica tiene incidencia directa en la confianza digital. Conforme el esquema de Indicadores de Confianza Digital 2019[648], la seguridad jurídica y tecnológica, la privacidad y la protección de datos personales son parte de los factores de que permiten evaluar un ecosistema digital sano. Por lo tanto, un marco regulatorio claro para responsables de tratamiento que establezca límites a sus actuaciones y desarrollos tecnológicos favorece la confianza digital. Asimismo, un ordenamiento jurídico adecuado incide de manera directa en la percepción positiva que las personas tienen del uso de internet, de los sistemas y las aplicaciones, lo que impulsa el comercio electrónico y de servicios.

   Asimismo, la seguridad jurídica se manifiesta en el reglamento cuando se establece que sus normas internas pueden ser especificadas o restringidas en la medida en que sea necesario "por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios", conforme el considerando (8) del RGPD; así como "reconoce un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de

---

[645] *Ibíd.*

[646] ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Informe sobre la economía digital 2019: creación y captura de valor: repercusiones para los países en desarrollo,* 04 de septiembre de 2019, accedido el 11 de noviembre de 2019.

[647] V. MILANÉS, *El sistema de protección de datos personales en América Latina: Oportunidades y desafíos para los derechos humanos*.

[648] OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN, *Esquema de Indicadores de Confianza Digital en España*, abril 2019, accedido el 12 de noviembre de 2019, https://www.ontsi.red.es/ontsi/sites/ontsi/files/2019-04/Esquema%20indicadores%20confianza%20digital%20%28abril%202019%29.pdf

datos personales («datos sensibles»), que determinen circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito", tal como señala el considerando (10) del RGPD. Finalmente, el tratamiento de datos personales para el cumplimiento de una obligación legal, de interés público o en ejercicio de poderes públicos conferidos al responsable del tratamiento, es posible si los Estados miembros están "facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del Reglamento" (considerando 10 citado previamente).

En el mismo sentido, aparece recogida esta postura en la LOPDGDD española que determina que pese a la aplicabilidad directa del RGPD:

> […] en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea (…) en suma, la elaboración de una nueva ley orgánica que sustituya a la actual. En esta labor se han preservado los principios de buena regulación, al tratarse de una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica.

h) *Libre circulación de datos:* El considerando 6 del RGPD determina que las personas físicas difunden cada vez más información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, por lo que se debe facilitar aún más la libre circulación de datos personales dentro de la Unión y a terceros países y organizaciones internacionales, y al mismo tiempo garantiza un elevado nivel de protección de los datos personales. Todo ello, debido a que el desarrollo tecnológico necesita de los datos personales para mejorar la entrega de bienes y servicios lo que influye directamente en el crecimiento de la economía digital. En este sentido, el citado reglamento europeo presenta el mandato expreso relativo a que "la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".[649]
i) *Flujos transfronterizos:* Por cuanto, el modelo económico, social y cultural europeo de intercambio de bienes y servicios incluidos los datos personales de sus ciudadanos; la globalización como fenómeno mundial que incrementa el intercambio de datos personales con países del resto del mundo; los avances tecnológicos y de análisis de información, así como el creciente intercambio de información entre las entidades públicas y privadas de distintos países, se evidencia la necesidad de un aumento sustancial de los flujos transfronterizos de datos personales como parte de la dinámica económica, así como para cumplir las obligaciones de cada Estado[650] de garantizar el ejercicio de sus derechos a sus ciudadanos como el disfrute de servicios públicos, eficientes y eficaces.
j) *Internet y la transformación digital de instituciones públicas y privadas:* Por su parte, la LOPDGDD española en su preámbulo señala que los datos personales "son

[649] *Ibíd.*
[650] RGPD, considerando (5) .

> el recurso fundamental de la sociedad de la información, que permite nuevos y mejores servicios, productos o hallazgos científicos" [651], pero también representa "riesgos, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso"[652]. En este sentido, normativas protectoras de derechos son la respuesta, empezando por la Declaración de los Derechos del Hombre y del Ciudadano en Internet, jurisprudencia especializada, hasta reglamentos de aplicación general y normas de transposición; que en conjunto, tienden a dotar de un marco jurídico consensuado y coherente para regular internet como espacio de libertades y ejercicio de derechos y además dotar a gobiernos y empresas de la guía y apoyo necesario para suscitar procesos de transformación digital que permitan acompasar la realidad mundial con la de los países de la región.

Luego de esta revisión básica, se colige que el reglamento europeo pretende desarrollar dos objetivos: el primero relativo al respeto de la dignidad humana, las libertades individuales en la era digital mediante el cumplimiento de los principios y normas relativas a la protección de los datos de carácter personal de todo ser humano sin discrimen de su nacionalidad o residencia. Al mismo tiempo, prevé un tratamiento de datos personales que contribuya "a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas".[653]

Como el objeto de este trabajo de investigación es identificar y analizar el contenido esencial del derecho a la protección de datos personales en los distintos modelos existentes, se ha realizado una descripción básica del entorno europeo que permite comprender el modelo de protección que impera en esta parte del mundo.

Para efectuar un análisis comparativo pertinente se debe tomar como base la normativa de vanguardia, la más avanzada[654], que contempla las últimas lecciones aprendidas en la comprensión y protección de este derecho fundamental, esto es el Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Para cumplir con la finalidad de la presente investigación se estudiará el contenido que explicite los elementos mínimos que a la luz del modelo europeo contiene el derecho a la protección de datos personales, en la visión global antes descrita; para lo cual se verificarán los elementos base y aquellas innovaciones que, en conjunto, permiten identificar las divergencias, mejoras y nuevas posturas que plantea el RGDP, así como varia precisiones

[651] LOPDGDD (preámbulo)
[652] *Ibíd.*
[653] RGPD.
[654] ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Informe sobre la economía digital 2019: creación y captura de valor: repercusiones para los países en desarrollo,* 04 de septiembre de 2019, accedido el 11 de noviembre de 2019, 12.

realizadas por tribunales y la adaptación que la legislación española ha realizado a través de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, LOPDGDD.

6.1 Ámbito

Respecto del ámbito, el RGPD establece una novedad al establecer dos niveles: ámbito material y ámbito territorial. Además, y de forma más ordenada, se establece los ámbitos de inaplicación, dentro del ámbito material; de esta forma se permite comprender con claridad el empleo de este conjunto de derechos y principios garantes del ser humano en la era digital.

6.1.1 Ámbito material

1. *Ámbito de aplicación:* EL RGPD señala en el artículo 2 el ámbito de aplicación material; es decir, explicita las características, condiciones y supuestos necesarios y propios que facultan un régimen de protección reforzado exclusivo de los datos personales, y por ende a qué tipo de dato, su naturaleza, las condiciones propias de este, los tipos de soporte, entre otros, a la que es aplicable el citado reglamento.

   A continuación las especificaciones constantes en el artículo 2 del RGPD:

   a) *Tratamiento automatizado o no automatizado de datos personales:* Se aplica este reglamento al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero[655]. Asimismo, el considerando (15) ibídem, señala que "A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas". Es decir, la condición primigenia es que se trate de datos personales, aquellos que identifican o hacen identificable a la persona. La automatización puede ser total o parcial y aun no estar automatizado siempre y cuando el destino de los datos sea incluirse en un fichero, dado que la recogida puede ser física, pero la organización y sistematización se formule en una base de datos, lo que ya es en sí mismo un mecanismo de tratamiento inicial.

   b) *Tratamiento de datos personales por las instituciones y los organismos comunitarios:* El Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas

[655] I*bíd.*

físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión[656] y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal. Se adaptarán a los principios y normas del RGPD de conformidad con su artículo 98 que se refiere a la posibilidad de la Comisión de revisar otros actos jurídicos de la Unión en materia de protección de datos y, de ser procedente, presentar propuestas legislativas para modificar otros actos jurídicos de la Unión en materia de protección de datos personales.

c) *Tratamiento de datos por parte de prestadores de servicios en actividades de comercio electrónico incluidos los prestadores de servicios intermediarios siempre y cuando cumplan lo señalado en el artículo 12 y 15 de la Directiva 2000/21:* Sin perjuicio de la aplicación de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), el RGPD se aplicará plenamente, incluidos los prestadores de servicios intermediarios siempre y cuando cumplan con las condiciones establecidas en sus artículos 12[657] y 15,[658] normas relativas a

[656] Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, accedido el 18 de diciembre de 2000, https://publications.europa.eu/es/publication-detail/-/publication/0177e751-7cb7-404b-98d8-79a564ddc629/language-es.

[657] "Artículo 12.- Mera transmisión. 1. Los Estados miembros garantizarán que, en el caso de un servicio de la sociedad de la información que consista en transmitir en una red de comunicaciones, datos facilitados por el destinatario del servicio o en facilitar acceso a una red de comunicaciones, no se pueda considerar al prestador de servicios de este tipo responsable de los datos transmitidos, a condición de que el prestador de servicios: a) no haya originado él mismo la transmisión; b) no seleccione al destinatario de la transmisión; y c) no seleccione ni modifique los datos transmitidos. 2. Las actividades de transmisión y concesión de acceso enumeradas en el apartado 1 engloban el almacenamiento automático, provisional y transitorio de los datos transmitidos siempre que dicho almacenamiento sirva exclusivamente para ejecutar la transmisión en la red de comunicaciones y que su duración no supere el tiempo razonablemente necesario para dicha transmisión. 3. El presente artículo no afectará a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exija al prestador de servicios que ponga fin a una infracción o que la impida". Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) EUR-Lex - 32000L0031 - ES, text/html; charset=UNICODE-1-1-UTF-8, Diario Oficial n° L 178 de 17/07/2000 p. 0001 - 0016, accedido 8 de septiembre de 2018, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:Es:HTML.

[658] "Artículo 15.- Inexistencia de obligación general de supervisión. 1. Los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios contemplados en los artículos 12, 13 y 14. 2. Los Estados miembros podrán establecer obligaciones tendentes a que los prestadores de servicios de la sociedad de la información comuniquen con prontitud a las autoridades públicas competentes los presuntos datos ilícitos o las actividades ilícitas llevadas a cabo por destinatarios de su servicio o la obligación de comunicar a las autoridades

la responsabilidad de dichos intermediadores, con el objetivo de contribuir al correcto funcionamiento del mercado interior y garantizar la libre circulación de los servicios de la sociedad de la información entre los Estados miembros (considerando 21, RGPD).

De esa manera, se distinguen tres tipos de tratamientos: los tratamientos transfronterizos (art. 4.23, RGPD); los transfronterizos pero con relevancia local en un Estado miembro (art. 56, RGPD), y aquellos exclusivamente nacionales (art. 55, RGPD).

Los artículos 1 y 2 del LGPD establecen la protección a los derechos fundamentales de libertad; privacidad; autodeterminación informativa; libertad de expresión, información, comunicación y opinión; inviolabilidad de la intimidad, honor e imagen; el desarrollo e innovación económica y tecnológica; la libre empresa, libre competencia y protección del consumidor; y los derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por parte de personas naturales. Asimismo, el artículo 17 del LGPD hace alusión a la titularidad de la persona sobre su dato, como atribución de sus poderes de decisión o control que son el reconocimiento de la autodeterminación informativa como garantía de los otros derechos citados.

2. *Ámbito de inaplicación:* Asimismo, no se aplica el Reglamento al *tratamiento de datos personales* que caigan en los siguientes supuestos (art. 2, RGPD):

    a) En el ejercicio de *una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión*, "como las actividades relativas a la seguridad nacional", conforme consta en el considerando 16, RGPD.

    b) Por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del Tratado de la Unión Europea (TUE);[659] es decir, relativa a la *política común de seguridad y defensa* que forma parte integrante de la política exterior y de seguridad común de la Unión Europea (considerando 16, RGPD); por la cual se ofrece a la Unión una capacidad operativa basada en medios civiles y militares para recurrir a dichos medios en misiones fuera de la Unión que tengan por objetivo garantizar el mantenimiento de la paz, la prevención de

competentes, a solicitud de éstas, información que les permita identificar a los destinatarios de su servicio con los que hayan celebrado acuerdos de almacenamiento". Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) EUR-Lex - 32000L0031 - ES.

[659] Tratado de Funcionamiento de la Unión Europea, versión consolidada.

conflictos y el fortalecimiento de la seguridad internacional, conforme a los principios de la Carta de las Naciones Unidas, conforme el artículo 42, TUE.

c) Efectuado por una persona física en el ejercicio de *actividades exclusivamente personales o domésticas*; al tenor de lo señalado en el considerando 18, RGPD, se entiende como actividades personales o domésticas, aquella que no guarda "conexión alguna con una actividad profesional o comercial, entre las cuales cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada fuera del contexto de las citadas actividades. No obstante, el Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas".

d) Por parte de las autoridades competentes con fines de *prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales*, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención. De conformidad con lo señalado en el considerando 19 del RGPD, si las autoridades públicas trataran datos personales deberán regirse a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.[660] Si el tratamiento de datos personales se realiza por parte de un organismo privado, "los Estados miembros puedan, en condiciones específicas, limitar conforme a Derecho determinadas obligaciones y derechos siempre que dicha limitación sea una medida necesaria y proporcionada en una sociedad democrática para proteger intereses específicos importantes, entre ellos la seguridad pública y la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, inclusive la protección frente a las amenazas contra la seguridad pública y su prevención. Esto se aplica, por ejemplo, en el marco de la lucha contra el blanqueo de capitales o de las actividades de los laboratorios de policía científica"; todo ello consta descrito en el considerando 19, RGPD.

[660] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) Documento DOUE-L-2016-80807, 680.

Cabe aclarar que, respecto de autoridades públicas, los datos con otras finalidades distintas a las señaladas en este literal, les son aplicables el presente RGPD. Asimismo, si dichas autoridades competentes tienen la posibilidad de mantener o introducir disposiciones más específicas para adaptar la aplicación de las normas del RGPD, como "requisitos concretos para el tratamiento de datos personales con otros fines, tomando en consideración la estructura constitucional, organizativa y administrativa de cada Estado" miembro (considerando 19, RGPD).

Aunque no constan en el artículo 2 del RGPD, existen varios casos especiales que afectan directamente al ámbito de aplicación del citado reglamento como son:

a) *Microempresas y las pequeñas y medianas empresas*:[661] Por las cuales, se incluye una serie de excepciones en materia de llevanza de registros para organizaciones con menos de 250 empleados. Además, se alienta a las instituciones y órganos de la Unión y a los Estados miembros y a sus autoridades de control a tener en cuenta sus necesidades específicas, al tenor de lo determinado en el considerando (13) del RGPD.

b) *Actividades de los tribunales y otras autoridades judiciales:* Conforme el considerando (20) del RGPD, l*a Función Judicial no se encuentra bajo el* cobijo del citado Reglamento como mecanismo que garantiza la independencia y no injerencia de autoridades administrativas en decisiones judiciales. Por este motivo, "en virtud del Derecho de la Unión o de los Estados miembros pueden especificarse las operaciones de tratamiento y los procedimientos de tratamiento, con la finalidad de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones. La competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del Reglamento, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos".[662]

---

[661] "Anexo.- Artículo 2.- Los efectivos y límites financieros que definen las categorías de empresas 1. La categoría de microempresas, pequeñas y medianas empresas (PYME) está constituida por las empresas que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones de euros o cuyo balance general anual no excede de 43 millones de euros. 2. En la categoría de las PYME, se define a una pequeña empresa como una empresa que ocupa a menos de 50 personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los 10 millones de euros. 3. En la categoría de las PYME, se define a una microempresa como una empresa que ocupa a menos de 10 personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los 2 millones de euros". COMISIÓN DE LAS COMUNIDADES EUROPEAS, Recomendación de la Comisión de 6 de mayo de 2003 sobre la definición de microempresas, pequeñas y medianas empresas. (L 124/36 Diario Oficial de la Unión Europea ES 20.5.2003, 20 de mayo de 2003), https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32003H0361&from=LT.

[662] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación

c) *Autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial:* Que conforme señala el considerando 31 corresponde a aquellas autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, quienes no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general. "Las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades públicas debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento".

6.1.2 Ámbito territorial

El RGPD en el artículo 3 señala el ámbito territorial, es decir, determina la territorialidad y extraterritorialidad del citado cuerpo normativo, al tenor de los siguientes criterios:

1. *Tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea, independientemente de si el tratamiento tiene lugar en la Unión o no:* El Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. Basta que el responsable o encargado, ya sea o no que utilice las modalidades de sucursal o filial con personalidad jurídica, "el ejercicio de manera efectiva y real de una actividad a través de modalidades estables" (considerando 22, RGPD).
   En el mismo sentido, "la STJUE en el "caso Weltimmo analiza el concepto fundamental de establecimiento y llega a la conclusión de que es aquel lugar donde se ejerce una actividad real y efectiva, aunque sea mínima pero en un contexto de estabilidad o de <<acuerdos estables con la UE>>".[663] Es decir, que realice sus actividades en cualquiera de los países miembros de la Unión Europea, sin importar que el tratamiento no se haga en dicho territorio, ni que los datos sean o no de ciudadanos europeos.

---

de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) Documento DOUE-L-2016-80807.

[663] F. GUDÍN RODRÍGUEZ-MAGARIÑO, *Nuevo Reglamento Europeo de Protección de Datos vs Big Data,* (Valencia: Tirant lo Blanch on line, 2018)

2. *Tratamiento de datos personales de Interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión:* El Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

   a) La oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago: De conformidad con el considerando 23, RGPD, se entiende que el responsable ofrece o proyecta ofrecer bienes o servicios al interesado que resida en la Unión, bajo los siguientes criterios: "el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión".[664] No es suficiente "la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento", [665] sino que estos criterios deberán unirse a otros factores para determinar la intención de ofrecer bienes o servicios.

   b) El control u observación del comportamiento del interesado, en la medida en que este tenga lugar en la Unión: Para lo cual se evaluará "si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes", al tenor de lo señalado en el considerando 24 del RGPD.[666]

   Se usa el término *interesado* precisamente para no excluir de este sistema de protección a una persona por su nacionalidad, y más bien el criterio vinculante es la residencia.

   c) Aplicación del Derecho Internacional Público: El Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público, por

[664] RGPD, considerando 23.
[665] *Ibíd*.
[666] *Ibíd.*

ejemplo en el caso de "una misión diplomática u oficina consular de un Estado miembro" (considerando 25, RGPD).[667]

De lo que se concluye que, a través del RGPD se puede proteger el derecho a la protección de datos personales más allá de las fronteras de la Unión Europea. Pues le es aplicable esta normativa, a todo establecimiento, entendido como entidad o empresa que en el contexto de sus actividades trate de datos personales, independientemente de si el tratamiento tiene lugar en la Unión o no. Asimismo, tendrá que cumplir con el contenido del RGPD y por ende con el adecuado tratamiento de datos personales de interesados que residan en la Unión, por parte de un responsable o encargado no establecido en la Unión; o que tenga que aplicar la normativa europea en virtud del Derecho Internacional Público.

6.2 Naturaleza del dato

La naturaleza del dato es parte del contenido esencial del derecho a la protección de datos personales, y conforme lo analizado previamente, su detalle suele estar recogido en las normas relativas al ámbito de aplicación o en aquellas referentes a las definiciones. En este sentido, se encuentra, además de su concepto general, varias precisiones indispensables para determinar sus alcances, dimensiones y aplicaciones en varias de las definiciones constantes en el artículo 4 del RGPD, del cual se partirá para el estudio:

1. *Datos personales:* El RGPD señala en el artículo 4, Definiciones: "A efectos del Reglamento se entenderá por: 1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

   Antecedentes de esta concepción que ahora se encuentra recogida en el RGPD constan en la sentencias de los casos *Lindqvist*, emitida el 6 de noviembre de 2003;[668] *Österreichischer Rundfunk* y otros, pronunciada el 20 de mayo del 2003;[669] Huber, expuesta el 16 de diciembre de 2008[670] y *Rijkeboer*, cuya emisión se dio el 7 de mayo del 2009.[671] Todas ellas resueltas por el Tribunal de Justicia de la Unión Europea, cuyas manifestaciones al definir dato personal

[667] *Ibíd*.
[668] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-101/01, en el caso: Lindqvist], 2003.
[669] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [En los asuntos acumulados C-465/00, C-138/01 y C-139/01, en el caso: Österreichischer Rundfunk y otros], 2003, accedido 13 de octubre de 2018, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62000CJ0465&from=HU.
[670] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-524/06, en el caso*: Huber*], 2008.
[671] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-553/07., en el caso: Rijkeboer], 2009, accedido 13 de octubre de 2018, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62007CJ0553.

descansan sobre el enunciado: “información sobre una persona física identificada o identificable”.

El considerando (26) aclara que los datos personales *seudonimizados,* que “cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable” y por lo tanto, dato personal.

El mismo considerando señala que para determinar “si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos”. Como la característica de identificable es de difícil comprensión, el RGPD determina en el considerando (26) la necesidad de los medios, en los que la singularización es uno de los que el responsable del tratamiento puede usar para volver a identificar a una persona, así como otros criterios como los costos y el tiempo, todo ello con el fin de demostrar la razonabilidad de los medios empleados, pues un exceso acarrea que el dato no sea considerado *seudonimizado*.

Coincide con esta observación lo dispuesto en el considerando (57) que determina que “si los datos personales tratados por un responsable no le permiten identificar a una persona física, el responsable no debe estar obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir cualquier disposición del Reglamento. No obstante, el responsable del tratamiento no debe negarse a recibir información adicional facilitada por el interesado a fin de respaldarle en el ejercicio de sus derechos. La identificación debe incluir la identificación digital de un interesado, por ejemplo mediante un mecanismo de autenticación, como las mismas credenciales, empleadas por el interesado para abrir una sesión en el servicio en línea ofrecido por el responsable”.

Asimismo, el considerando (30) señala que “las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas”.

Por ello, respecto de datos personales inocuos, que son aquellos que no tienen la consideración de íntimos porque se consideran superficiales; basta con la condición de que identifiquen o hagan identificable a una persona, están bajo la égida de la protección de datos personales como derecho fundamental.

Para ello, no basta atender únicamente al tipo de datos exigidos; lo decisivo en la Jurisprudencia del tribunal constitucional federal alemán es su utilidad y la posibilidad de emplearlos. Esto depende, de una parte, de la finalidad a la que sirve la encuesta, y de la otra, de las posibilidades de procesamiento y vinculación propias de la tecnología de la información. De ese modo, un dato que por sí mismo puede ser visto como insignificante puede adquirir valor; es así como bajo las condiciones del procesamiento automático de datos deja de haber datos "insignificantes". Qué tan sensibles son las informaciones, no dependerá sólo del hecho de que toquen asuntos íntimos. Para determinar el significado de un dato respecto del derecho de la personalidad se requiere conocer el contexto en que va a ser utilizado: sólo cuando existe claridad sobre la finalidad para la que se recauda la información y sobre las posibilidades que existen de utilizarla y relacionarla, podrá responderse si una restricción al derecho a la autodeterminación de la información es admisible. Al respecto, se tiene que diferenciar entre los datos vinculados a la persona, que son recolectados y procesados en forma individual, no anónima (al respecto, vid. infra, inciso "a"), y aquellos que se han determinado con fines estadísticos (al respecto, vid. infra, inciso "b").[672]

Sobre datos anónimos, el considerando (26) del RGPD señala que "los principios de protección de datos no deben aplicarse a información anónima, es decir aquella que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación". Por lo que, este tipo de datos se entiende por fuera del sistema de protección ya que no ponen en riesgo la dignidad humana.

Sobre datos personales que se recopilan para fines estadísticos se aclara que:

Una encuesta, de la persona, realizada con fines estadísticos, puede ser vista, por consiguiente, como contraria a la dignidad y como una amenaza al derecho de autodeterminación cuando abarca la esfera de la vida propia del ser humano, que por naturaleza tiene el carácter de secreta, y convierte ese núcleo íntimo en

[672] Alemania, TRIBUNAL CONSTITUCIONAL FEDERAL, "Sentencia de la Primera Sala, del 15 de diciembre, 1983, BVerfGE 65, 1 [Censo de Población]", *Jurisprudencia del tribunal constitucional federal alemán: Extractos de las sentencias más relevantes compilados por Jürgen* Schwabe, Editor: R. HUBER, (Fundación Konrad Adenauer, A.C.: México, 2009), 96.

material accesible y susceptible de ser valorado estadísticamente. En esta medida también para el Estado de la sociedad industrial moderna existen límites frente a la "despersonalización" técnico-administrativa. Donde, por el contrario, la encuesta estadística vincule sólo el comportamiento del ser humano en el mundo externo, ésta no abarca la personalidad humana en su ámbito inviolable de la conformación de la vida privada. Esto es válido en todo caso siempre y cuando esas informaciones pierdan la relación con la persona mediante el anonimato de su valoración. El presupuesto para esto es que el anonimato se encuentre suficientemente asegurado [...]"[673]

Finalmente, el considerando (26) del RGPD aclara que los principios de la protección de datos deben aplicarse a todo dato personal, como ya se revisó aquel considerado íntimo pero también el superficial e inocuo. Quedan excluidos los datos anónimos ya sea que hayan sido recopilados con fines históricos o estadísticos pues no vinculan a la persona determinada y por lo tanto pierden la condición de identificar o hacerla identificable.

2. *Tratamiento:* El RGPD señala en el artículo 4, Definiciones: "A efectos del Reglamento se entenderá por: [...] 2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción". La precisión que consta en esta norma hace referencia a que se pueden tratar no solo datos personales, sino conjuntos de datos personales.

3. *Tratamiento transfronterizo:* El artículo 4, numeral 23, señala la definición de tratamiento transfronterizo, entendido como aquel tratamiento de datos personales realizado:

    a. Si el responsable o el encargado está establecido en más de un Estado miembro.

    b. Si el tratamiento de datos personales afecta o es probable que afecte sustancialmente a interesados en más de un Estado miembro.

4. *Limitación del tratamiento:* El RGPD señala en el artículo 4, Definiciones: "A efectos del Reglamento se entenderá por: [...] 3) «limitación del tratamiento»: el

[673] Alemania, TRIBUNAL CONSTITUCIONAL FEDERAL, "Sentencia BVerfGE 27, Sentencia de la Primera Sala, del 16 de julio, 1969, [Microcenso] Sobre la constitucionalidad de una estadística representativa (microcenso)", *Jurisprudencia del tribunal constitucional federal alemán: Extractos de las sentencias más relevantes compilados por Jürgen Schwabe,* Editor: R. HUBER, (Fundación Konrad Adenauer, A.C.: México, 2009), 93.

marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro".

5. *Elaboración de perfiles:* El RGPD señala en el artículo 4, Definiciones: "A efectos del Reglamento se entenderá por: [...] 4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales". El tratamiento automatizado, esto es sin intervención humana consiste en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación, situación o movimientos de dicha persona física, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar, al tenor del considerando (71) del RGPD.

6. *Seudonimización:* El RGPD señala en el artículo 4, Definiciones: "A efectos del Reglamento se entenderá por: [...] 5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

   El uso y aplicación de la seudonimización a los datos personales "puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos", al tenor de lo señalado en el considerando (28) del RGPD.

   El considerando (29) señala la posibilidad de establecer medidas de seudonimización en el tratamiento de datos personales, por parte de los responsables del tratamiento, como un mecanismo para incentivar la aplicación de la seudonimización. Al mismo tiempo que permite un análisis general, cuando este haya adoptado medidas técnicas y organizativas necesarias para garantizar la aplicación del RGPD al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas.

7. *Fichero:* El RGPD señala en el artículo 4, Definiciones: "A efectos del Reglamento se entenderá por: [...] 6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

8. *Datos genéticos*[674]: El RGPD señala en el artículo 4, Definiciones: "A efectos del Reglamento se entenderá por: [...] 13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona".

   El considerando (34) del RGPD determina que "debe entenderse por datos genéticos los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente".

   La importancia que han tomado los datos genéticos es indudable, dado que responde a un "desarrollo tecnológico que permite tomar al cuerpo humano como fuente de información. De tal suerte, los avances en tecnología genética para la prevención y tratamiento de enfermedades, para estimar riesgos para la salud o para establecer lazos biológicos han sido significativos".[675] Sin duda la investigación científica basada en datos genéticos abre una puerta para solucionar varios problemas de salud pública, así como, para realizar avances científicos que pueden repercutir en otras áreas de la ciencia. Sin embargo, también se plantea un debate ético-jurídico, pues la obtención de estos datos, su tratamiento, puede poner en riesgo a sus titulares, sobre todo porque a través de esta información pudiera llegarse a discriminar a quien debido a sus condiciones genéticas ha sido categorizado con algún criterio que lo segrega negativamente.

   Es tan compleja esta temática, que el artículo 9, numeral 4 del RGPD deja a los Estados miembros de la Unión la posibilidad de mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud, atendiendo a las propias experiencias y condiciones de cada país.

9. *Datos biométricos:* El RGPD señala en el artículo 4, Definiciones: "A efectos del Reglamento se entenderá por: [...] 14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

[674] J. APARICIO SALOM, *Estudio sobre la protección de datos* (Cizur Menor, Navarra: Aranzadi, 2013), 126.
[675] V. MILANÉS, *Op.cit.*

Respecto de si una fotografía se considera dato biométrico, el considerando (51) señala que: "El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física". Es decir, para que una fotografía pueda servir como dato biométrico debe someterse a un procesamiento digital que permita la extracción de los puntos de identificación y la aplicación de criterios de comparación con un vector original, pues solo en estas condiciones se puede identificar a una persona.

Su importancia radica en las nuevas y distintas formas de implementación de tecnologías de reconocimiento biométrico, pues estos datos "han comenzado a ser recolectados y usados en una cada vez mayor variedad de contextos, principalmente como medio de identificación y autenticación".[676] De ahí que, como se analizó previamente, serán los Estados miembros de la Unión los que podrán definir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de este tipo d datos, artículo 9, numeral 4 del RGPD.

10. *Tratamiento de categorías especiales de datos personales:* El RGPD recoge varios criterios de protección en relación con el tratamiento de categorías especiales de datos personales, es decir de datos sensibles. El RGPD no utiliza esta nomenclatura en el articulado, sino que lo desarrolla en los considerandos; el número (10) señala expresamente a los datos sensibles como una categoría especial de datos personales, y el considerando (51) aclara que "especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico".

En el artículo 9 relativo al tratamiento de categorías especiales de datos personales constan varios criterios de protección reforzada: el primero es el más importante y por el cual "1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexuales de una persona física". Efectivamente, este tipo de información podría afectar al sujeto en todos los ámbitos de su vida e impedirle un adecuado desarrollo social, profesional, familiar, político, entre otros.

[676] V. MILANÉS, *Op.cit.*

Si bien, la normativa señala la prohibición de tratamiento para datos personales que revelen categorías sospechosas, entendidas aquellas que de conocerse o difundirse pueden llegar a causar discriminación.

> Existen esferas que requieren ser mantenidas en reserva, por ejemplo la investigación de la paternidad, o el tema de las adopciones. La vida amorosa y las relaciones de amistad, que incluye la vida sexual y, por extensión los embarazos prematrimoniales. El ámbito de las comunicaciones personales, que comprende las diferentes vías de comunicación como las epistolares, telefónicas, electrónicas, fax, etc. La situación económica personal, referidas al nivel de ingreso, patrimonio, inversiones, y obligaciones financieras. [677]

De lo citado anteriormente, se advierte que por el concepto de datos sensibles se entiende a los datos íntimos según la cultura de cada lugar o tiempo.[678]

El considerando (51) señala que la protección especial a la que hace alusión este tipo de datos se refiere a que no deben ser tratados a menos que se permita su tratamiento en situaciones específicas contempladas en el RGPD o por normas específicas de cada Estado que establezcan específicamente una excepción, o una obligación legal o el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. También, entre otros aspectos, cuando el interesado dé su consentimiento explícito, en especial para actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales. Se aclara, además, que le son aplicables no solo los requisitos específicos de ese tratamiento, sino los principios generales y otras normas del RGPD, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento.

Si bien, el tratamiento de datos sensibles esta proscrito, sin embargo existen condiciones que habilitan su tratamiento a modo de excepción, las mismas que se analizarán a continuación:

a) *Consentimiento explícito:* Se pueden tratar datos sensibles si el interesado otorga su consentimiento explícito, excepto cuando el Derecho de la Unión Europea o de cada Estado miembros establezca expresamente que la prohibición no puede ser levantada por el interesado, artículo 9, literal a) RGPD.

---

[677] K. MEDINACELI, *El tratamiento de los datos sanitarios en la historia clínica electrónica: Caso boliviano* (Madrid: Agencia Española de Protección de Datos, 2017), 224.

[678] COMITÉ JURÍDICO INTERAMERICANO DE LA OEA, *Informe Privacidad y Protección de Datos Personales No. CJI/doc. 474/15 rev.2*, Rio de Janeiro, 26 de marzo de 2015, accedido el 2 de noviembre de 2019, http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_documentos_referencia_CJI-doc_474-15_rev2.pdf

b) *Derechos laborales y de seguridad y protección social:* Se puede tratar datos sensibles si el tratamiento es necesario para el "cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado" (art. 9, lit. b), RGPD). El RGPD desarrolla esta excepción, pues señala en el considerando 155 que la normativa de "los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral".

c) *Intereses vitales propios o de otros:* Es posible el tratamiento de datos sensibles cuando es necesario "para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento" (art. 9, literal c), RGPD).

d) *Organismos sin fin de lucro:* Está facultado el tratamiento cuando es efectuado, en el ámbito de actividades legítimas y con debidas garantías, por parte de una "fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados" (art. 9, lit. d), RGPD).

e) *Datos manifiestamente notorios:* Es posible el tratamiento de datos sensibles si el interesado los ha hecho manifiestamente públicos (art. 9, lit. e), RGPD).

f) *Defensa en juicio o ejercicio de la función judicial:* Es posible el tratamiento de datos sensibles para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial (art. 9, lit. f), RGPD).

g) *Medicina preventiva y laboral:* El tratamiento es posible si es necesario para "fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de

tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social". Se incluyen los casos en los que el tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, o por cualquier otra persona sujeta también a la obligación de secreto (art. 9, lit. h), RGPD).

h) Interés público en el ámbito de la salud: Está facultado el tratamiento de datos sensibles por razones de interés público en el ámbito de la salud pública para la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios (art. 9, lit. i), RGPD). Por su parte, el considerando (53) establece que "las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social".

Entretanto, el artículo 4 RGPD, señala que debe entenderse por datos de salud bajo las siguientes consideraciones: "Artículo 4.- Definiciones: A efectos del Reglamento se entenderá por: [...] 15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".

Por su parte, el considerando (35) del RGPD incluye entre las características que estos sean pasados, presentes o futuros, así como "la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo;[679] a todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro".

[679] Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza, s. f., 2.

i) Datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos: El tratamiento de datos personales sensibles es posible cuando es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, siempre que se cumpla lo dispuesto en el artículo 89, apartado 1, RGPD y la normativa de la Unión o de sus Estados miembros. En otras palabras, que sea proporcional al objetivo perseguido, se respete lo esencial del derecho a la protección de datos y se establezcan medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. En el mismo sentido, el RGPD señala las condiciones propias que deben cumplirse en el tratamiento para cada una de estas finalidades, contempladas en el artículo 89, cuando indica las garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, entre las que constan expresamente: 1. Sujetas a las garantías adecuadas, con arreglo al Reglamento, para los derechos y las libertades de los interesados, en especial medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo; 2. Se podrán limitar los derechos de acceso, rectificación, cancelación y oposición, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines; 3. En el mismo sentido que el anterior, pero referidos a datos personales con fines de archivo en interés público.

Por su parte, el considerando (156) determina que este tipo de datos debe supeditarse a unas garantías adecuadas para los derechos y libertades del interesado como: a) aplicar medidas técnicas y organizativas, en particular, el principio de minimización de los datos, atendiendo a los principios de proporcionalidad y necesidad; b) el tratamiento ulterior de datos personales ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un "tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos)"; c) establecer, especificaciones y excepciones en la normativa interna con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, incluidos procedimientos específicos a la luz de los fines perseguidos por el tratamiento específico; d) establecer normas específicas con vistas a salvaguardar el deber de secreto profesional u obligaciones equivalentes, en la medida necesaria para conciliar el derecho a la protección de los datos personales con el deber de secreto profesional,

considerando (164); y, e) los poderes de las autoridades de control para obtener del responsable o del encargado del tratamiento acceso a los datos personales y a sus locales debe constar en la normativa interna de cada estado miembro, dentro de los límites fijados por RGPD, sin perjuicio de las normas sobre el secreto profesional, considerando (164).

El considerando (51) señala que la protección especial a la que hace alusión este tipo de datos se refiere a que no deben ser tratados a menos que se permita su tratamiento en situaciones específicas contempladas en el RGPD o por normas específicas de cada Estado que establezcan específicamente una excepción, o una obligación legal o el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o, entre otras cosas, cuando el interesado dé su consentimiento explícito, en especial para actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales. Se aclara además que le son aplicables no solo los requisitos específicos de ese tratamiento, sino los principios generales y otras normas del RGPD, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento.

Asimismo, además de estas condiciones generales de aplicación, cada finalidad establece cuestiones propias que se analizan a continuación:

i. *Tratamiento de datos personales con fines de archivo en interés público:* El considerando (158) determina que el RGPD debe aplicarse al tratamiento de datos personales realizado con fines de archivo, teniendo presente que no se aplique a personas fallecidas. “Las autoridades públicas o los organismos públicos o privados que llevan registros de interés público deben ser servicios que están obligados, a adquirir, mantener, evaluar, organizar, describir, comunicar, promover y difundir registros de valor perdurable para el interés público general y facilitar acceso a ellos. Los Estados miembros también debe estar autorizados a establecer el tratamiento ulterior de datos personales, con fines de archivo, por ejemplo, a fin de ofrecer información específica relacionada con el comportamiento político bajo antiguos regímenes de Estados totalitarios, el genocidio, los crímenes contra la humanidad, en particular el Holocausto, o los crímenes de guerra”.

ii. *Tratamiento de datos personales con fines de investigación científica:* El considerando (159) señala que el tratamiento de datos personales con fines de investigación científica debe interpretarse “de manera amplia [...] que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. [...] Entre los fines de

investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública".

Por su parte, el considerando (157) señala que "los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión de la combinación de información procedente de registros. Los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales. Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, cumpliendo ciertas condiciones y garantías adecuadas".

a) Las condiciones propias de esta finalidad radican en "la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del Reglamento deben aplicarse teniendo en cuenta tales medidas" (considerando [159]).

b) El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos (considerando [156]), en especial las relacionadas con el consentimiento para la participación en este tipo de actividades, conforme el Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo (considerando [161]).

iii. *Tratamiento de datos personales con fines de investigación histórica:* El RGPD se aplica al tratamiento datos personales que se realiza con fines de investigación histórica incluida la investigación histórica y la investigación para fines genealógicos, no se aplica a personas fallecidas (considerando [160]).

iv. *Tratamiento de datos personales con fines estadísticos:* El considerando (162) señala que "el contenido estadístico, el control de accesos, las especificaciones para el tratamiento de datos personales con fines

estadísticos y las medidas adecuadas para salvaguardar los derechos y las libertades de los interesados y garantizar la confidencialidad estadística", deben ser específicamente establecidas en la normativa interna de cada país miembro, y además proteger la información confidencial de las autoridades estadísticas tanto de la Unión como de cada país miembro conforme la normativa internacional como nacional (considerando [163]).

Para clarificar la temática, el mismo considerando (162) señala que "por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos. Estos resultados estadísticos pueden además utilizarse con diferentes fines, incluidos fines de investigación científica. El fin estadístico implica que el resultado del tratamiento con fines estadísticos no sean datos personales, sino datos agregados, y que este resultado o los datos personales no se utilicen para respaldar medidas o decisiones relativas a personas físicas concretas".

La Sentencia BVerfGE 27 sobre microcenso señala la complejidad y la importancia de los datos estadísticos, pues si bien proceden de titulares, es necesario recabarlos para obtener información que permita una eficiente toma de decisiones de política pública, que satisfaga las necesidades de la población. Ahora bien, en dicha resolución se analiza porque los datos personales que se obtienen de los censos pueden significar un riesgo para su titular, de tal manera que:

> La falta de un vínculo a un fin determinado, reconocible en todo momento y realizable, así como el empleo multifuncional de los datos, fortalecen las tendencias a que esto se regule y restrinja mediante leyes para la protección de datos personales, que concreten el derecho garantizado constitucionalmente a la autodeterminación de la información. Debido a que desde un principio faltan límites que derivan de la sujeción a un fin determinado, los censos de población llevan consigo tendencialmente el peligro ya subrayado en la sentencia sobre el microcenso (BVerfGE 27,1 [6]), de un registro en contra de la personalidad y de una categorización del individuo. Incluso para la recolección de datos individuales que serán utilizados con fines estadísticos, el legislador debe examinar –al establecer un deber de informar– si para los implicados se puede generar el peligro de un etiquetamiento (por ejemplo, como "adicto a las drogas", "persona con antecedentes criminales", "enfermo mental", "persona asocial", etc.) y si el objetivo de la encuesta no puede lograrse mediante una investigación anónima. [680]

[680] Alemania: TRIBUNAL CONSTITUCIONAL FEDERAL, "Sentencia BVerfGE 27, 1 Sobre la constitucionalidad de una estadística representativa (microcenso), de la Primera Sala, del 16 de julio, 1969 –1 BvL 19/63-", *Jurisprudencia del tribunal constitucional federal alemán: Extractos de las sentencias más relevantes*

> Sin embargo, y tal como sostiene el considerando (162) del RGPD, si la obtención de datos puede alcanzarse sin necesidad de aportar información que pueda vincularse directamente a personas en forma individual, que por lo tanto no haga posible el etiquetamiento social, es posible recabarla y tratarla. Ya que, datos estadísticos que contienen datos personales anónimos son una forma efectiva, adecuada y respetuosa de derechos humanos de obtener información para la generación de una adecuada política pública, fin último de un censo. Anotándose que, estos datos estadísticos pueden ser puestos a disposición de otros órganos estatales o instituciones especiales sin restricciones a través de transferencias de datos que no requieren autorización del titular ni de la ley. Pero si los datos, por algún motivo, aún guardan relación con su titular, estos no tendrán la condición de estadísticos, y tampoco serán anónimos, por lo que en este caso no sería posible el tratamiento ni la comunicación, y el hacerlo significa una transgresión al derecho a la protección de datos personales.[681]

j) Tratamiento de datos personales relativos a condenas e infracciones penales: En el artículo 10 del RGPD se señala que el tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas, siempre y cuando el titular haya dado consentimiento explícito para uno o varios fines específicos (art. 6, num. 1, RGPD) únicamente "podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas".

k) Tratamiento que no requiere identificación: El artículo 11 del RGPD señala que si para los fines para los cuales un responsable trata datos personales no se requiere o ya se no requiere identificación de un interesado, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el Reglamento. Si el responsable es capaz de demostrar que no está en condiciones de identificar al interesado lo informará de ser posible, y por ende no podrá viabilizar el ejercicio de derechos ARCO, a menos que el interesado, a

---

compiladas por Jürgen Schwabe, compilador: R. HUBER, (Fundación Konrad Adenauer, A.C.: México,2009), 99.

[681] Alemania: TRIBUNAL CONSTITUCIONAL FEDERAL, "Sentencia BVerfGE 27, 1 Sobre la constitucionalidad de una estadística representativa (microcenso), de la Primera Sala, del 16 de julio, 1969 –1 BvL 19/63-", *Jurisprudencia del tribunal constitucional federal alemán: Extractos de las sentencias más relevantes compiladas por Jürgen Schwabe,* compilador: R. HUBER, (Fundación Konrad Adenauer, A.C.: México,2009), 99.

efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

l) Tratamiento en Interés público esencial: Es plausible el tratamiento de datos sensibles por razones de un interés público esencial, siempre y cuando esté amparado por normativa de la Unión o de cada Estado miembro; y sea proporcional al objetivo perseguido, respete el derecho a la protección de datos y establezca medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado (art. 9, lit. g), RGPD).

Ahora bien, la frase interés público es muy amplia porque puede incluir cuestiones previamente analizadas como aquellas relativas a seguridad del Estado, salud pública, enfermedades epidemiológicas, protección social, gestión de servicios públicos o incluso aquellos relativos a la investigación de infracciones administrativas o penales, que incluyen lavado de activos, financiamiento de terrorismo, evasión tributaria o aduanera, o lucha contra la corrupción, entre las más destacadas.

Se anota que debido a la importancia de este tipo de información para la paz, la armonía social y la subsistencia de la democracia y del estado de derecho, no es relevante el formato en el que se encuentren los datos personales, pudiéndose encontrar en muchos casos en formato físico. En estos casos sea necesaria su digitalización con formato interoperable para que pueda ser usado.

Ahora bien, el intercambio de información entre instituciones públicas no se justifica por el solo hecho de corresponder al interés público sino que deben estar previsto en un ley o política pública que establezca el cumplimiento de derechos o deberes estatales, para lo cual se podrá revisar en los estatutos de conformación de las instituciones públicas, las funciones o competencias asignadas a cada una de ellas.

Finalmente, "el sector público ha comenzado a solicitar o requerir al sector privado la retención y entrega de información personal determinada, sea a través de una orden legal o con fines de política pública".[682]

En suma, se deberá promover un intercambio de datos personales que permita cumplir o mejorar la provisión de servicios y operaciones, así como la optimización de trámites, a través de un procesamiento de datos personales más eficiente. Para lo cual será necesario el cumplimiento de los principios del tratamiento, entre los que destaca la calidad del dato, ya que solo a través de información confiable se puede garantizar un adecuado

[682] V. MILANÉS, *Op. cit. Cit.*

cumplimiento de los fines institucionales y la adecuada atención a los derechos del ciudadano.

6.3 Sujeto activo

El sujeto activo es el titular del derecho, específicamente la persona natural, pero no las personas jurídicas; en particular, no se aplica el RGPD a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto, y tampoco a empresarios individuales. Únicamente es aplicable esta normativa, sus derechos, principios y normas a la persona natural.

Anotándose que, en los considerandos (2) y (14) del RGPD y en el capítulo III se usa la frase "derechos de los interesados"; es decir, se utiliza el término "interesado".

La ley no habla de titular del dato sino de interesado, por lo tanto "se podrá incluir, a mi entender, a todas aquellas actuaciones que, derivadas del tratamiento de datos de carácter personal, puedan afectar a personas que un momento determinado no estén en condiciones de ejercer los derechos que establece la LOPDGDD. En este caso el interesado no sería el titular de los datos pero estaría legitimado para ejercer los derechos de las personas vinculadas a ella y que no estén en condiciones de hacerlo".[683]

Es decir, con la finalidad de que no exista requisito previo que deba ostentar el titular, como la condición de ciudadanía o de nacionalidad previamente obtenida, se omiten, de tal manera que no resulte determinante, sino que sea suficiente la condición humana para cumplir con el objetivo en sí mismo de este derecho, el de respetar las libertades y derechos fundamentales de un individuo, en particular el derecho a la protección de los datos de carácter personal. A lo sumo en el ámbito de aplicación se requiere que el interesado sea residente de un país de la Unión Europea.

Según el considerando (27) el RGPD tampoco se aplica al tratamiento de los datos personales de fallecidos. No obstante, es conveniente resaltar en estos momentos que el artículo 3 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establece claramente que las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión, salvo que la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley (en cualquier caso, dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante).

[683] G. FREIXAS GUTIÉRREZ, *La protección de los datos de carácter personal en el derecho español*, 122.

Respecto de un grupo de especial protección como son los niños, el considerando (38) del RGPD determina un rango de protección específica de sus datos personales, ya que "pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños".

El titular debe comprender la importancia de este derecho, ya que sus datos personales son su manifestación digital. No son un parte de un imaginario, un alter ego o una intelectualización sino que son la persona misma en entornos virtuales.

> Debe partirse del hecho de que uno de las premisas básicas de la nueva normativa consiste en devolver al ciudadano el empoderamiento sobre sus propios datos de carácter personal. Cuando se menciona el término "empoderamiento", se está haciendo referencia a la devolución a toda persona de la capacidad de decidir de manera efectiva, sobre la disposición y el control de dichos datos, de modo y manera que pueda determinar en cada momento quien puede tratar tales datos, y a qué fin o fines está autorizado para destinar dicho tratamiento. Ello constituye una realidad tangible dentro de nuestro ámbito social y jurídico.[684]

Este empoderamiento hace referencia al ejercicio de los titulares de su derecho a la autodeterminación informativa, tanto en el mundo *on line* como *off line*. De ahí que sea tan importante que el sujeto activo dimensione de forma adecuada la aplicabilidad del derecho a la protección de datos personales, para que, ante el constante desarrollo tecnológico y social, pueda afrontar y defenderse de situaciones que no ha previsto y ni siquiera imaginado aún.

6.4 Sujeto pasivo

El RGPD establece varios sujetos pasivos, que son aquellos a quienes la citada norma constriñe y solicita el cumplimiento de obligaciones específicas y, en caso de no cumplirlas, responsabiliza directamente, incluso con indemnizaciones si se llegaren a producir daños por su acción u omisión. El considerando (74) del RGPD estipula que "debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el

[684] E. DELGADO CARAVILLA, J. PUYOL MONTERO, *La implantación del nuevo Reglamento General de Protección de Datos de la Unión Europea, (Valencia: Tirant Lo Blanch on line, 2018)*

contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas".

Los sujetos pasivos son:

a) *Responsable de tratamiento o simplemente "responsable"*: La definición de responsable consta en el artículo 4, numeral 7) del RGPD y determina que es "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento".

   En la definición de responsable el RGPD hace una determinación interesante, pues establece que si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, este mismo derecho podrá establecer el responsable de tratamiento o los criterios específicos para su nombramiento, conforme el citado artículo 4, literal 7. De esta manera podrá ser la ley la que establezca quien es el responsable de tratamiento en virtud de ciertos fines o medios de tratamiento que le son atribuibles por sus competencias o atribuciones, por ejemplo.

   Conforme la STS español, 3 de diciembre de 2002, recurso No. 7050/2001 respecto de las características que definen al responsable del fichero, dice: "es quien decide sobre la finalidad, contenido y uso del tratamiento automatizado y no quien le facilita el dato en virtud de un contrato celebrado con aquel, de modo que solo el responsable del fichero está sujeto al régimen sancionador."

b) *Encargado del tratamiento o simplemente "encargado":* La definición de encargado consta en el artículo 4, numeral 8) del RGPD y determina que es "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

   El artículo 28, numeral 3, señala que el tratamiento por parte del encargado de tratamiento se regirá por un contrato u otro acto jurídico que cumpla con la normativa de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, las obligaciones y derechos del responsable incluida la confidencialidad.

c) Destinatario: La definición de destinatario consta en el artículo 4, numeral 9) del RGPD que establece: "la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento".

d) *Tercero:* La definición de encargado consta en el artículo 4, numeral 9) del RGPD que establece que es: *"*la persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado".

El artículo 4, literal 16 del RGPD, además de establecer a los sujetos activos establece varias definiciones que ayudan con las dudas respecto de la aplicación de esta normativa.

a) *Establecimiento principal:* A efectos de comprender a quienes cobija la categoría de responsables, el artículo 4, numeral 16, establece que se entenderá como establecimiento principal:

i. *Respecto de un responsable del tratamiento,* con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal.

ii. *Respecto de un encargado del tratamiento,* con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al RGPD.

b) *Representante:* El artículo 4, numeral 17, establece que se entenderá como representante a la "persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones".

Para tal efecto deberá cumplirse con lo dispuesto en el artículo 27 del RGPD; es decir, se deberá cumplir con los siguientes supuestos cuando se realice tratamiento de datos personales por oferta de bienes o servicios, o para el control del comportamiento de interesados de datos por parte de responsables o encargados no establecido en la Unión.

i. *Designar por escrito un representante:* El responsable o el encargado del tratamiento designará por escrito un representante en la Unión, también lo hará el responsable o el encargado del tratamiento no establecido en la Unión que esté tratando datos personales de interesados que residan en la

Unión y cuyas actividades de tratamiento están relacionadas con la oferta de bienes o servicios, independientemente de si se requiere un pago por parte de estos, o con el control de su comportamiento en la medida en que este tenga lugar en la Unión. A menos que: a) el tratamiento sea ocasional y no incluyan datos sensibles ni relativos a condenas e infracciones penales, ni grandes volúmenes de datos (considerando [80]) del RGPD y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o b) sea proveniente de autoridades u organismos públicos.

El mismo considerando (80) del RGPD señala que el representante debe desempeñar sus funciones conforme al mandato recibido del responsable o del encargado, incluida la cooperación con las autoridades de control competentes y estar sujeto a medidas coercitivas en caso de incumplimiento por parte del responsable o del encargado.

ii. *Establecido en país de interesados cuyos datos se están tratando:* El representante estará establecido en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado.

iii. *Obligado a atender consultas de interesados y de autoridad de control:* El responsable o el encargado del tratamiento encomendará al representante que atienda, junto al responsable o al encargado, o en su lugar, a las consultas, en particular, de las autoridades de control y de los interesados, sobre todos los asuntos relativos al tratamiento, a fin de garantizar el cumplimiento de lo dispuesto en el RGPD.

iv. *Acciones contra representantes y contra el propio responsable o encargado:* La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

c) El artículo 4, numeral 18, establece que se entenderá como empresa: Esto es la "persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica".

d) El artículo 4, numeral 19 del RGPD, establece que se entenderá como «grupo empresarial», entendido como "el grupo constituido por una empresa que ejerce el control y sus empresas controladas". El considerando (37) señala que un grupo empresarial debe estar "constituido por una empresa que ejerce el control y las empresas controladas, debiendo ser la empresa que ejerce el control la que pueda ejercer una influencia dominante en las otras empresas, por razones, por ejemplo, de propiedad, participación financiera, normas por las que se rige, o

poder de hacer cumplir las normas de protección de datos personales. Una empresa que controle el tratamiento de los datos personales en las empresas que estén afiliadas debe considerarse, junto con dichas empresas".

e) El artículo 4 numeral 20) del RGPD determina que las normas corporativas vinculantes "son políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta".

La relación entre el responsable y el encargado está determinada en el considerando (81) del RGPD, puesto que consta expresamente que respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, deberá encomendar las actividades de tratamiento únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, que apliquen medidas técnicas y organizativas, incluida la seguridad del tratamiento. Además, será necesaria la celebración de un contrato u otro acto jurídico, incluida la adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado para que pueda realizarse el tratamiento por parte de un encargado, siempre y cuando se regule el objeto y la duración del tratamiento, la naturaleza, fines del tratamiento, la devolución o eliminación de los datos una vez cumplido el encargo, el tipo de datos personales y las categorías de interesados, con una clara determinación de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado.

Debido a que en la normativa española de protección de datos personales, se reconocen los llamados derechos digitales[685], podemos señalar que por su diversidad, la determinación de los sujetos pasivos de cada uno de ellos, depende de su contenido específico. De lo que debemos recalcar que la protección de datos personales es uno de los derechos digitales cuyos sujetos pasivos, han sido analizados previamente.

> Nos encontramos, por tanto, en un momento todavía incipiente en cuanto a la definición, extensión y regulación de estos derechos digitales destacando su heterogeneidad (mientras que algunos son auténticos derechos digitales, otros son manifestaciones de derechos ya existentes en el mundo físico y mientras que algunos tienen el carácter de derechos y libertades fundamentales (los recogidos en el título I, capítulo II, sección I de la Constitución, arts. 14 a 29) otros son derechos ordinarios). También tenemos que mencionar aquellos derechos digitales que se asimilarían más bien a los principios rectores de la política social y económica recogidos en el capítulo III del título I de la Constitución, en concreto en los arts. 39 a 52, o incluso a derechos que no son tales, como el denominado

[685] Consideramos como derechos digitales propiamente dichos aquellos derecho que carecen de contenido fuera del ámbito de Internet. COMISIÓN JURÍDICA DEL CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA, Informes 2018, (Valencia: Tirant Lo Blanch, 2019), 21

> "derecho al testamento digital", que se refieren más bien a procedimientos para que determinadas personas autorizadas puedan eliminar el contenido de personas fallecidas en las redes sociales. Además hay que referirse a la disparidad de los sujetos obligados en cada caso, dado que en ocasiones lo son los proveedores de servicios de Internet (es decir, las operadoras de telecomunicaciones), otras veces son los Poderes Públicos, en otros supuestos los proveedores de servicios tecnológicos (entre ellos las grandes multinacionales tecnológicos como Google o Facebook) o los medios de comunicación convencionales o digitales o incluso otros ciudadanos. Es evidente que por buenas que sean las intenciones del legislador en cuanto a las garantías de los derechos digitales habrá que tener en cuenta que en la práctica tropezará con las dificultades derivadas de los distintos sujetos obligados o de los términos de los acuerdos y contratos que se hayan firmado con los proveedores de servicios, incluso aunque podamos denunciar que, en la mayoría de los casos, estamos- al menos para el usuario final- ante contratos de adhesión.[686]

Tal como ocurre con el derecho a la protección de datos personales, los sujetos pasivos de los derechos digitales son aquellos que cumplen con ciertas condiciones, características o relaciones señaladas por la ley. En tal virtud, los sujetos pasivos están obligados a cumplir con preceptos que garantizan el respeto a la dignidad de los titulares del derecho. Dada la actual realidad de transgresiones a las personas en entornos virtuales, es preferible hablar de derechos digitales para que el resguardo no se centre en el cumplimiento o incumplimiento contractual desde una perspectiva acotada del titular como mero consumidor.

6.5 Objeto o bien jurídico

6.5.1 Derecho de información

EL RGPD aborda el derecho de información en el capítulo III, titulado derechos del interesado, bajo la sección 1, denominada transparencia y modalidades, cuyo artículo 12 no hace referencia al nombrado derecho de información, sino a la transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado, aunque su contenido termina siendo lo mismo. Bajo esta perspectiva el responsable del tratamiento tomará las medidas oportunas para facilitar información al interesado relativo al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios (art. 12, num. 1, RGPD).

El antecedente que versa sobre la importancia de este derecho se encuentra recogido en la sentencia del caso Bara y otros, emitida el 1 de octubre de 2015 y resuelta por el Tribunal

[686] COMISIÓN JURÍDICA DEL CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA, *Op. cit. Cit*., 21

de Justicia de la Unión Europea; en ella, este último, manifiesta que la "exigencia de información de los interesados resulta especialmente importante en la medida en que es una condición necesaria para el ejercicio por éstos de su derecho de acceso a los datos objeto de tratamiento y de rectificación de los mismos".[687]

Si bien este derecho tiene su contraparte en el deber de información del responsable del tratamiento, por el cual este último debe cumplir una serie de obligaciones con la finalidad de garantizar el derecho de información del titular.

La información deberá ser remitida de forma gratuita; podrá transmitirse en combinación con iconos normalizados, incluso legibles mecánicamente, que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto (art. 12, num. 5, RGPD).

La generación de vías más efectivas de información para el individuo, que sea clara, concisa y pertinente y le posibilite la comprensión acabada de la suerte de sus datos personales es todavía materia pendiente. Especial atención merecen los mecanismos y herramientas que posibiliten la efectiva implementación, aplicación y control de las protecciones y garantías (*enforcement)*, que han aparecido como una de las principales deficiencias y obstáculos para el desarrollo de los sistemas de protección de datos personales.[688]

6.5.2 Autodeterminación informativa

Como se vio en el numeral 4 de este capítulo segundo, el objeto de la protección de datos personales es el derecho a la autodeterminación informativa.

La Sentencia BVerfGE 65, sobre Censo de Población realiza un análisis sobre la autodeterminación informativa como derecho fundamental y reconoce que debido a los avances de las Tic, el registro, almacenaje y tratamiento de los datos personales de un individuo pueden afectarlo directamente, no solo desde la perspectiva del honor, la imagen o la intimidad sino directamente sobre el libre desarrollo de su personalidad y el ejercicio de sus libertades individuales porque todas las actividades, preferencias, gustos, acciones pueden organizarse, sistematizarse y en suma asignarles categorías que podrían en algún momento segregar al individuo apartándolo de la sociedad, asignándole juicios de valor, o peor aún discriminándolo.

[687] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C201/14, en el caso: Bara y otros], 2015, accedido 13 de octubre de 2018, file:///Users/biblioteca/Downloads/Dialnet-TribunalDeJusticiaDeLaUnionEuropeaCronicaDeJurispr-5466803.pdf.
[688] V. MILANÉS, O*p cit.. Cit.*

> La autodeterminación individual presupone –también bajo las condiciones de la moderna tecnología para el procesamiento de información– que a los individuos se les dé libertad para decidir sobre qué actividades emprender y cuáles omitir, incluyendo la posibilidad de comportarse efectivamente de conformidad con esa decisión. Quien no pueda estimar con suficiente seguridad, qué informaciones sobre sí mismo son conocidas en determinadas esferas de su medio social, y quien no pueda de algún modo valorar el conocimiento previo que los posibles interlocutores tienen de uno mismo, puede verse restringido esencialmente en su libertad para planear o decidir con base en su propia autodeterminación. Un ordenamiento social y un orden legal en el que los ciudadanos no pudieran conocer quiénes, cuándo y en qué circunstancias saben qué sobre ellos, serían incompatibles con el derecho a la autodeterminación de la información. Quien piense que los comportamientos atípicos pueden en todo momento ser registrados y archivados como información, utilizados o retransmitidos, intentará no llamar la atención incurriendo en ese tipo de comportamientos. Quien crea que, por ejemplo, la participación en una asamblea o una iniciativa ciudadana será registrada por las autoridades y que ello pueda generarle algún riesgo, posiblemente renunciará al ejercicio de su derecho fundamental (Arts. 8, 9 de la Ley Fundamental). Esto no sólo iría en detrimento de las posibilidades de desarrollo individual de los individuos, sino también de la comunidad, porque la autodeterminación es una condición funcional elemental de una nación democrática libre, fundada en la capacidad de sus ciudadanos para cooperar y actuar. De esto se deduce lo siguiente: el libre desarrollo de la personalidad presupone en las modernas condiciones para el procesamiento de datos, la protección de los individuos frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales. Esa protección se contempla en los derechos fundamentales previstos en el Art. 2, párrafo 1, en relación con el Art. 1, párrafo 1 de la Ley Fundamental. El derecho fundamental garantiza de esta manera la capacidad del individuo principalmente para determinar la transmisión y empleo de sus datos personales. b) Este derecho a la "autodeterminación de la información" no se garantiza ilimitadamente. El individuo no tiene un derecho en el sentido de un señorío ilimitado, absoluto, sobre "sus" datos; el individuo es ante todo una personalidad que se desarrolla en el interior de una comunidad social y que está obligada a la comunicación. La información, en la medida que también está vinculada a la persona, representa una imagen de la realidad social, la cual no puede atribuirse de manera exclusiva sólo a los implicados. Como se ha subrayado reiteradamente en la jurisprudencia del Tribunal Constitucional Federal, la Ley Fundamental ha decidido la tensión que existe entre el "individuo" y la comunidad destacando la referencia y vinculación de la persona con la comunidad (BVerfGE 4, 7 [15]; 8, 274 [329]; 27,1 [7]; 27, 344 [351 y ss.]; 33, 303 [334]; 50, 290 [353]; 56, 37 [49]). El individuo debe admitir ciertas restricciones a su derecho a la autodeterminación de la información, principalmente en aras del interés general preponderante." [689]

La autodeterminación informativa se traduce entonces en la libertad que tienen las personas de decidir todos los aspectos relacionados a sus datos personales, no solo los considerandos

[689] Alemania: TRIBUNAL CONSTITUCIONAL FEDERAL "Sentencia BVerfGE 65, 1 [Censo de Población], de la Primera Sala, del 15 de diciembre, 1983", *Jurisprudencia del tribunal constitucional federal alemán: Extractos de las sentencias más relevantes compiladas por Jürgen Schwabe*, Compilador: R. HUBER, (Fundación Konrad Adenauer, A.C.: México, 2009), 96.

especiales, sino cualquiera de estos sean, inclusive los inocuos, irrelevantes y hasta los metadatos.

La autodeterminación informativa como parte del contenido esencial del derecho a la protección de datos personales, como se vio previamente, tiene su origen en la jurisprudencia. En líneas preliminares se analizaron varias sentencias. Ahora solo se mencionarán las más sobresalientes: a) la sentencia sobre el censo demográfico, dictada el 15 de diciembre de 1983 del Tribunal Constitucional Federal Alemán,[690] por la cual se determina que la "facultad del individuo de decidir básicamente cuándo y dentro de qué límites procede relevar situaciones referentes a la propia vida, haciendo necesaria la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitadas de los datos concernientes a la persona";[691] b) la sentencia española STC 254/1993, de 20 de julio, señala por primera vez la existencia de un derecho a la protección de los datos personales, por el cual el titular tiene el derecho de control sobre sus datos; c) la sentencia de la STC 124/1998, de 15 de junio, consagra un derecho fundamental autónomo e independiente de controlar el flujo de informaciones que le conciernen a cada persona para así preservar el pleno ejercicio de otros derechos fundamentales, como en este caso que se afectó un derecho laboral de un funcionario de RENFE; y, la sentencia alemana BVerfGE 106, sobre grabación de conversaciones telefónicas señala que:

> […] junto con el derecho a la propia imagen– el derecho a la palabra hablada (cf. BVerfGE 34, 238 [246s.]; 54, 148 [154]). Con ello se garantiza la autodeterminación sobre la manera en que la persona se presenta a sí misma en la comunicación con otros (cf. BVerfGE 54, 148 [155]). Esta protección abarca la posibilidad de comportarse –en el proceso de comunicación– en forma adecuada a las circunstancias (tomando como referencia la propia valoración), y de adaptarse según los interlocutores presentes. También forma parte del derecho fundamental el que cada quien pueda determinar por sí mismo si el contenido de la comunicación debe ser accesible únicamente al interlocutor, a un determinado grupo de personas o al público en general (cf. BVerfGE 54, 148 [155] haciendo referencia a BGHZ 27, 284 [286]; cf. también BAGE 41,37 [42], así como –adhiriéndose a dicha resolución– BGH, NJW 1991, p. 1180). El derecho de autodeterminación se extiende, pues, a la elección de las personas que puedan tener acceso al contenido de una conversación. Este derecho de autodeterminación encuentra un modelo de expresarse en la potestad de la persona de decidir por sí misma si su voz puede ser almacenada en una grabadora, de modo que posiblemente pueda hacerse accesible a terceros. (…) Por el contrario, la comunicación humana debe ser protegida por el derecho fundamental para evitar que las palabras –quizá una expresión poco ponderada o espontánea, una postura meramente transitoria adoptada en el marco de una conversación en desarrollo, una formulación que sólo pueda ser comprendida cabalmente dentro de una determinada situación–, sacadas de su contexto o empleadas en una ocasión distinta puedan ser utilizadas –atendiendo a su contenido, a la

[690] Alemania: TRIBUNAL CONSTITUCIONAL FEDERAL, [Sentencia de 15 de diciembre de 1983, BJC 33, IV Jurisprudencia Constitucional Extrajera], 1984.
[691] C. RUIZ MIGUEL, *El derecho a la protección de la vida privada en la Jurisprudencia del Tribunal Europeo de Derechos Humanos* (Madrid: Civitas, 1994), 50.

> forma de expresarlas o al tono en que fueron dichas– en contra del emisor. Por tanto, la Ley Fundamental protege al individuo de que sus conversaciones se sean grabadas secretamente y sean utilizadas sin el consentimiento o incluso contra la voluntad declarada del emisor […]"[692]

En el RGPD no existe alusión expresa a la autodeterminación informativa debido a que este contenido esencial es parte del derecho a la protección de datos personales, que es concebido como: un mecanismo para regular el tratamiento de datos personales; el respeto a otros derechos fundamentales; libertades y principios reconocidos, en particular el respeto de la vida privada y familiar; del domicilio y de las comunicaciones; la libertad de pensamiento; de conciencia y de religión; la libertad de expresión y de información; la libertad de empresa; el derecho a la tutela judicial efectiva y a un juicio justo; y, la diversidad cultural, religiosa y lingüística.

El RGPD determina que para que sea posible una protección adecuada a la autodeterminación informativa y debido al desarrollo acelerado de nuevas tecnologías y lo complejo de su aplicación en muchos casos, solo es posible una adecuada salvaguarda si es que se asigna a un delegado de protección de datos personales que en virtud de sus funciones asesore, alerte e impida de ser el caso la transgresión de este derecho.

La utilización de los datos está limitada a los fines determinados por la ley. En vista de los peligros que presenta el procesamiento automático de datos, se requiere de una protección (frente a las posibles desviaciones de los fines) que prohíba la retransmisión y el reciclaje de los datos –incluso frente a la posibilidad de que una autoridad pretenda obligar a otra a proporcionar determinada información. Adicionalmente, es esencial regular disposiciones de carácter procedimental que contemplen el deber de aclaración, de información y de eliminación de información de las bases de datos. Debido a la poca claridad que existe para el ciudadano sobre el archivo y empleo de los datos bajo las condiciones del procesamiento automático de los mismos, y también en aras de una protección jurídica anticipada a través de medidas adoptadas oportunamente, resulta bastante significativa la participación de un funcionario independiente, encargado de la protección de la información para la protección efectiva del derecho a la autodeterminación de la información. [693]

Finalmente, la importancia del derecho a la autodeterminación informativa en la era digital es la continua interrelación de este derecho con otros derechos humanos. Y es que, la cotidianeidad de las personas ahora se realiza en Internet de tal manera que, sobre la

---

[692] Alemania: TRIBUNAL CONSTITUCIONAL FEDERAL "Sentencia BVerfGE 106, 28 [Grabación de conversaciones telefónicas], de la Primera Sala, del 9 de Octubre, 2002 - 1 BvR 1611/96, 1 BvR 805/98", *Jurisprudencia del tribunal constitucional federal alemán: Extractos de las sentencias más relevantes compiladas por Jürgen Schwabe*, Compilador: R. HUBER, (Fundación Konrad Adenauer, A.C.: México,2009), 96.

[693] Alemania, TRIBUNAL CONSTITUCIONAL FEDERAL, "Sentencia de la Primera Sala, del 15 de diciembre, 1983, BVerfGE 65, 1 [Censo de Población]", *Jurisprudencia del tribunal constitucional federal alemán: Extractos de las sentencias más relevantes compiladas por Jürgen Schwabe,* (Fundación Konrad Adenauer, A.C.: México,2009), 99.

información personal, que en realidad es la persona misma en su manifestación digital, pueden suscitarse una serie de circunstancias que lo pongan en riesgo. Incluso podemos decir que a través de los datos personales de un individuo se pudiera llegar afectar no solo la autodeterminación informativa sino o el catálogo de derechos humanos.

> Generar mecanismos dinámicos y multiparticipativos que permitan identificar y contener los riesgos generados por los avances tecnológicos. La generación de canales y mecanismos dinámicos y con participación de referentes de los diversos sectores involucrados (funcionarios de protección de datos, sector privado y técnico, academia y sociedad civil) aparece como necesaria para la adecuada identificación, comprensión, contención y conciliación de estas circunstancias, y la consecuente generación de alternativas coherentes con el derecho de autodeterminación informativa. Propiciar instancias de interacción y diálogo para el fortalecimiento de la autodeterminación informativa y su confluencia con otros derechos humanos. La contundencia del derecho a la autodeterminación informativa, en tanto garantiza al individuo el control de sus datos, genera innumerables y permanentes situaciones de conflicto con otros derechos, también esenciales para su adecuado desarrollo. Más allá de las vías procedimentales y judiciales, en las que en última instancia transcurrirán y se resolverán los conflictos en cuestión, la generación de espacios de interacción y diálogo que posibiliten el debate riguroso, experto y permanente de las diversas situaciones de confluencia de los derechos en cuestión posibilitará la generación de *expertise* e insumos que redunden en un fortalecimiento del ejercicio del derecho a la auto determinación informativa como parte integrante del conjunto de derechos humanos del individuo.[694]

6.5.3 Necesidad de mandato legal para tratamiento sin autorización del titular

La piedra angular del sistema de protección de los datos personales es el consentimiento que podía ser suplido por el legislador, quien justificadamente emitía una norma que autorizaba el tratamiento de datos personales sin permiso del titular.

La derogada Directiva 95/46, en el título denominado principios relativos a la legitimación del tratamiento de datos, contemplaba en el artículo 7 que el tratamiento solo podía efectuarse con consentimiento previo del interesado, ejecución de un contrato o para la aplicación de medidas precontractuales, cumplimiento de una obligación jurídica, proteger el interés vital del interesado, cumplimiento de una misión de interés público o inherente al ejercicio del poder público, o satisfacción de un interés legítimo.

El RGPD, en el artículo 6 sobre la licitud del tratamiento menciona un cambio que se verifica en el título de este capítulo. Ya no se trata de la legitimación como consta en la anterior Directiva, sino de la licitud del tratamiento; es decir, que la ley determina cuándo es lícito y, por lo tanto, legítimo un tratamiento.

Las condiciones que establece el RGPD para determinar la licitud del tratamiento coinciden en su mayoría con aquellas que constaban en la citada Directiva. Se mejora su contenido como aquel por el cual el tratamiento es necesario para el cumplimiento de una

[694] V. MILANÉS, O*p cit.. Cit.*

obligación legal aplicable al responsable del tratamiento. También se realizan ciertas precisiones como la que se refiere al consentimiento, puesto que ahora la norma prevé el consentimiento para el tratamiento para uno o varios fines específicos. Y la relativa a la satisfacción de intereses legítimos en el que se añade aquel previsto en el caso particular en el que el interesado sea un niño.

Asimismo, es posible el tratamiento sin autorización del titular, pero por autorización legal para: la ejecución de un contrato, en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; el cumplimiento de una obligación legal aplicable al responsable del tratamiento; proteger intereses vitales del interesado o de otra persona física; el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. (artículo 6 RGPD)

Respecto de "interés legítimo" en la sentencia del caso ASNEF, emitida el 24 de noviembre de 2011 por el Tribunal de Justicia de la Unión Europea, se establecen "dos requisitos para que un tratamiento de datos personales sea lícito". Se hace constar "por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o los terceros a los que se comuniquen datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado".[695]

La base del tratamiento y la finalidad deberá constar de forma específica en la normativa pertinente cuando se verifica para el cumplimiento de una obligación legal o de una misión de interés público o inherente al ejercicio del poder público y será proporcional al fin legítimo perseguido. Se determinará en especial las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas.

Finalmente, cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en disposición legal que lo autorice en su lugar, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta la relación entre los fines previos y ulteriores; el contexto en que se hayan recogido los datos personales; la naturaleza de los datos personales, en concreto las categorías especiales de datos personales; las posibles consecuencias para los interesados del

[695] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, "En los asuntos acumulados C-468/10 y C-469/10, en el caso: ASNEF", 2011, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/document/document.jsf?docid=115205&doclang=ES

tratamiento ulterior previsto; y, finalmente, la existencia de garantías adecuadas que podrán incluir el cifrado o la seudonimización (art. 6, RGPD).

6.5.4 Principios

El artículo 5 del RGPD reconoce varios principios propios del tratamiento de datos personales, los cuales se analizarán a continuación. Varios de ellos corresponden en contenido a los recogidos en la normativa latinoamericana especializada, pero con otras denominaciones. Por ejemplo, se tiene el principio de calidad que en el texto europeo aparece como exactitud; o el caso del principio de transparencia que se recoge como derecho o deber de información en otras legislaciones.

En ese contexto, resulta imperante empezar por reconocer la serie de principios que serán aquí analizados. Así, los tres primeros que se traerá a mención forman parte del artículo 5 literal a), correspondiendo a la licitud, lealtad y transparencia. A partir de ello, en el RGPD el apartado dedicado a *Principios* es el que se encarga de su desarrollo, de tal manera que inicia con el de finalidad, en el cual se determina que la serie de características a la que esta debe atender para mantenerse en apego a los márgenes de este reglamento, es que debe ser determinada, explícita y legítima. Y, conjuntamente, exterioriza la prohibición de un tratamiento ulterior incompatible con las finalidades iniciales, siempre que el interés público, fines de investigación científica e histórica o fines estadísticos no las contradicen.

Además, se determina que los datos deben ser adecuados, pertinentes y limitados en concordancia con las finalidades previamente establecidas; así también, exactos y actualizados con la opción de someterse a un proceso de rectificación de no cumplir con ello; en el mismo panorama, podrán conservarse durante un lapso no superior al necesario para garantizar el cumplimiento de las finalidades exceptuando aquellas destinadas al archivo en interés público, fines de investigación científica o histórica o fines estadísticos; se añade, que deben ser tratados garantizando índices adecuados de seguridad mediante la aplicación de medidas técnicas u organizativas apropiadas, concluyendo con la categoría de responsabilidad proactiva que asumirá el responsable respecto de la aplicación de lo dispuesto.

6.5.4.1 Deber de información

El RGPD aborda el deber de información desde la perspectiva de obligaciones que el responsable de tratamiento debe cumplir. En la discusión de si se trata de un derecho, el RGPD se decanta por calificarlo como un principio.[696] Conforme el considerando (39) del

[696] "No se trata realmente de un derecho, sino de un principio que, como tal, debe ser respetado por el titular del fichero o tratamiento, de esta forma podemos hablar de la recogida de datos en forma leal, entendiendo por tal la necesidad de que, en todo caso, el interesado pueda estar en condiciones de conocer que se están

RGPD desde la perspectiva del derecho de información, el titular tiene derecho a ser informado; y desde la visión de obligación, el responsable tiene el deber de informar respecto de los riesgos, la finalidad, las normas, las salvaguardas y los derechos y la forma de hacer valer estos derechos en relación con el tratamiento.

Sin embargo, desde el enfoque del derecho de acceso los titulares de tratamiento tienen derecho a "conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento", al tenor de lo señalado en el considerando (63) del RGPD.

De acuerdo con lo prescrito en el artículo 12 del RGPD, el responsable del tratamiento debe tomar las medidas oportunas para facilitar al interesado la siguiente información:

1. *Información y acceso a los datos personales que deberá facilitarse cuando los datos personales se obtengan del interesado:* El artículo 13 del RGPD señala que cuando se obtengan datos personales, el responsable del tratamiento, en el momento de la recogida, le facilitará toda la información indicada a continuación, incluida aquella necesaria para garantizar un tratamiento de datos leal y transparente:

    a. La identidad y los datos de contacto del responsable y, en su caso, de su representante.
    b. Los datos de contacto del delegado de protección de datos.
    c. Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
    d. La constancia de que el tratamiento lícito es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, al tenor de lo señalado en el artículo 6, apartado 1, literal f) del RGPD.
    e. Los destinatarios o las categorías de destinatarios de los datos personales.
    f. La intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación, o, en el caso de las transferencias mediante garantías adecuadas, normas corporativas vinculantes y a los medios para obtener una copia de estas o al hecho de que se hayan prestado, al tenor de lo indicado en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo del RGPD.
    g. El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
    h. El consentimiento explícito del interesado sobre el tratamiento con las finalidades específicas, incluso en el caso de categorías especiales de datos, de conformidad con el artículo 6, apartado 1, letra a), y el artículo 9,

recabando los datos y su finalidad o consecuencias del tratamiento, así como quién es el titular responsable del mismo y en qué lugar puede ejercer los derechos que le asisten". M. DAVARA RODRÍGUEZ, *Manual de Derecho Informático*, 87.

apartado 2, letra a); o cuando sea o no posible autorizar tratamiento de datos sensibles, se informará sobre el derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

i. La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.
j. El derecho a presentar una reclamación ante una autoridad de control.
k. La expresa mención de que la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos.
l. La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, incluida información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de dicho tratamiento.
m. La decisión del responsable del tratamiento de proyectar el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron; tal información se proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, determinando el otro fin propuesto y cualquier información adicional pertinente.

2. *Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado:* El artículo 14 señala que cuando los datos personales no se hayan obtenido del interesado directamente, el responsable del tratamiento debe cumplir con entregar la mayoría de la información necesaria cuando los datos personales se han obtenido del mismo titular, más aquella propia que se detalla a continuación, incluida aquella necesaria para garantizar un tratamiento de datos leal y transparente:

a. La identidad y los datos de contacto del responsable y, en su caso, de su representante.
b. Los datos de contacto del delegado de protección de datos.
c. Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
d. Las categorías de datos personales de que se trate.
e. Los destinatarios o las categorías de destinatarios de los datos personales.
f. La expresa mención de la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación, o, en el caso de las transferencias mediante garantías adecuadas, normas corporativas vinculantes y a los medios para obtener una copia de estas o al hecho de que se hayan prestado, al tenor de lo indicado en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo del RGPD.

g. El plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo.
h. La mención respecto de si el tratamiento lícito es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, al tenor de lo señalado en el artículo 6, apartado 1, literal f) del RGPD.
i. La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.
j. El consentimiento del interesado para fines específicos, incluidos el de categoría especiales de datos, de conformidad con el artículo 6, apartado 1, literal a), es o el artículo 9, apartado 2, literal a); o cuando sea o no posible autorizar tratamiento de datos sensibles, se informará sobre el derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.
k. El derecho a presentar una reclamación ante una autoridad de control.
l. La fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.
m. La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, incluida información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de dicho tratamiento.
n. El responsable del tratamiento facilitará la información anterior:
    i. Dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos.
    ii. Si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado.
    iii. Si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.
o. La constancia de la intención del responsable de proyectar un tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, y además proporcionar al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente.
p. Las disposiciones antes referidas no serán aplicables cuando y en la medida en que:
    i. el interesado ya disponga de la información;
    ii. la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1; o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda

imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

iii. la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado

iv. Por su parte, el considerando (62) del RGPD señala los casos en los que no es necesario cumplir con el deber de información, y por las cuales no es necesario imponer la obligación de proporcionar información: a) cuando el interesado ya posea la información; b) cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley; c) cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. "Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas".

q. Cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional incluida una obligación de secreto de naturaleza estatutaria.

r. La información podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente (art. 12, RGPD).

3. *Derechos de acceso, rectificación, supresión, limitación del tratamiento, obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento, derecho a la portabilidad de los datos personales, derecho de oposición y sobre decisiones individuales automatizadas, incluida la elaboración de perfiles:* El responsable del tratamiento está obligado a entregar información respecto de la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos, conforme lo prescrito en los artículos 13 y 14 del RGPD.

   Adicionalmente, el artículo 12 del RGPD señala que el responsable no se negará a actuar a petición del interesado, salvo que pueda demostrar que no está en condiciones de identificarlo. Sin perjuicio de que determinado tratamiento no requiera identificación, cuando el responsable tenga dudas razonables en relación con la identidad de la persona física, podrá solicitarle que se facilite la información adicional necesaria para confirmar su identidad como peticionario.

El responsable del tratamiento facilitará la información relativa a sus actuaciones, con base en lo establecido en los artículos 15 a 22 (relativos a los derechos de acceso, rectificación, supresión, etc.), en el plazo de un mes a partir de la recepción de la solicitud. Tomando en cuenta la complejidad y el número de solicitudes el plazo, podrá prorrogarse por dos meses; estas prórrogas deberán informarse al interesado en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos de ser posible, a menos que el interesado solicite que se facilite de otro medio.

Si la respuesta es negativa informará en el plazo de mes contado desde la recepción las razones de su no actuación y de su derecho de presentar una reclamación ante una autoridad de control y de ejercitar otras acciones judiciales.

Toda información se facilitará a título gratuito. Sin embargo, cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

i. cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada;
ii. negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

4. *Sobre la violación de la seguridad de los datos personales:* Conforme señala el artículo 34 del RGPD, si la violación de seguridad de los datos personales puede entrañar un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida, en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales, y contendrá como mínimo la información y las medidas descritas en el artículo 33, apartado 3, literales b), c) y d); esto es:

i. comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
ii. describir las posibles consecuencias de la violación de la seguridad de los datos personales;
iii. describir las medidas adoptadas o propuestas por el responsable para remediar la violación de seguridad, incluyendo si proceden las medidas adoptadas para mitigar los posibles efectos negativos.

La comunicación sobre una vulneración de seguridad de los datos personales no será necesaria si se cumple alguna de las condiciones siguientes:

i. el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
ii. el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concrete el alto riesgo para los derechos y libertades del interesado;
iii. suponga un esfuerzo desproporcionado; en este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

Si el responsable no ha comunicado la violación de seguridad, la autoridad de control, verificada que esta puede acarrear un alto riesgo, podrá exigir al responsable la debida notificación.

Según el análisis del RGPD efectuado, el deber de información se ha desarrollado ampliamente, estableciendo una serie de obligaciones para los responsables de tratamiento. De primera vista, pareciera una carga de compromisos y de acciones que modifican la interrelación titular del dato y responsable del tratamiento. Sin embargo, estas precisiones aquí citadas mejoran la transparencia de la relación, contribuyen al respeto, empoderan al ciudadano y establecen una serie de garantías que deben ser implementadas por el responsable que puede tener la certeza de que los datos personales que utiliza para el giro de sus actividades cumplen con los mayores estándares y evita la posibilidad de trasgresión

6.5.4.2 Pertinencia, adecuación y minimización de datos

Una referencia de la concepción actual del principio de pertinencia, adecuación y minimización de datos, que ahora se encuentra recogido en el RGPD, consta en la sentencia del caso *Google Spain y Google*, emitida el 13 de mayo de 2014, resuelta por el Tribunal de Justicia de la Unión Europea, en el cual este último menciona que "incumbe al responsable del tratamiento garantizar que los datos personales sean adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y se traten posteriormente".[697]

En conformidad con lo anterior, el RGPD en el artículo 5 relativo a los principios sobre el tratamiento señala: "1. Los datos personales serán: [...] c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)". Es decir, reconoce a la pertinencia como uno de los principios aplicables a la

[697] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, "Asunto C-131/12, en el caso: Google Spain y Google", 2014, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES.

protección de datos personales, aunque acompañado con otros principios que serán analizados también en su conjunto.

a) *Principio de dato adecuado, pertinente y no excesivo:* Si bien esta referencia no se encuentra desarrollada en los considerandos del RGDP, en la normativa española constaba en el numeral 1 del artículo 4 de la derogada LOPD, que textualmente dice: "Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". Y lo mismo determina el artículo 8.1 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (esta norma sí se encuentra aún en vigor): "4. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

   Este principio a primera vista no reviste complicaciones, ya que "antes de proceder a recabar los datos de trabajadores, clientes o proveedores para incorporarlos a sus ficheros, sean automatizados o no, ha de delimitar con precisión cual va a ser la finalidad de los mismos para, de esta forma, solicitar únicamente aquellos que sean necesarios para su cumplimiento. Por ejemplo, si para crear un Fichero de Clientes con la finalidad de enviarles publicidad de productos o servicios, se solicita su DNI, este dato sería inadecuado en relación con la finalidad determinada y legítima para la que fue obtenido, pues carece de relevancia a efectos publicitarios".[698]

   Sin embargo, la determinación de la finalidad de un fichero es problemática, aun cuando el diseño supone una estrategia concreta para la consecución de un objetivo específico, como por ejemplo: un programa de fidelización basado en la atención al cliente, a través del Call Center, con el que se pretende disminuir la tasa de pérdida de clientes en un determinado porcentaje. Las amplias determinaciones no permiten la identificación concreta de la finalidad para la cual se está recabando un dato. En consecuencia, no se puede evaluar si el dato es adecuado, pertinente y no excesivo.
   Por cuanto, el principio de adecuación y pertinencia va de la mano de otros principios como el de finalidad y el de consentimiento informado e inequívoco, los responsables de tratamiento deben cumplir con el principio de calidad de datos para lo cual deberán recabar el consentimiento informado e inequívoco de los titulares de los datos con la finalidad específica de que se tratarán sus datos para elaborar las tarjetas de perfil y calificación de cliente, por ejemplo.

[698] N. SÁNCHEZ MOURIS, "Los datos personales en el inicio de la actividad empresarial", Directoras: ANA MARZO PORTERA Y FERNANDO MA. RAMOS SUÁREZ, *La Protección de Datos en la Gestión de Empresas,* cit., p. SÁNCHEZ MOTRIZ, "Capítulo 2. Los datos personales en el inicio de la actividad empresarial, 53.

Además, el considerando 39 del RGPD al referirse a la pertinencia, adecuación y minimización de datos señala que para garantizar el cumplimiento de estos principios se requerirá de "medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento"; es decir, todos los principios se encuentran íntimamente interrelacionados, de tal manera que, la transgresión de uno comprende la de otro, como si de un juego de dominó se tratare no solo por su interrelación fáctica, sino sobre todo porque el resultado concreto es una transgresión a la protección del dato personal y por ende a su titular.

b) *Minimización de datos:* Sobre este tema, tanto el citado artículo 5.1, literal c) del RGPD señala que es un principio que va de la mano de la pertinencia y la adecuación; pero además en el considerando 39 del RGPD señala que para que este principio se cumpla se "requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica". Como se puede concluir de la cita, la minimización no es un principio cuya aplicación se refiera exclusivamente a la recogida de datos sino que atiende a todo el ciclo del dato, es decir su tratamiento, uso y destrucción, de tal manera que en conjunto se demuestre que el responsable minimiza su interacción con el dato en garantía de los derechos de las personas, pero también desde el punto de vista del responsable del tratamiento, que le signifique un trabajo ordenado, organizado y eficiente que le permita una rentabilidad del dato al mismo tiempo que no le signifique gastos innecesarios.

c) *Limitación del plazo de conservación:* Concordante con la minimización de datos, el RGPD recoge otro principio relacionado con el tiempo de interacción entre el responsable del tratamiento y el dato en sí mismo. Ya que el artículo 5.1, literal e), señala que los datos personales "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»)". Se verifica que existe un incentivo directo a trabajar más con datos seudoanonimizados y, aún más, con datos anónimos, de tal manera que los esfuerzos se dirigirán a desarrollar tecnologías anonimizadas que permitan a los responsables tratar y usar este tipo datos.

6.5.4.3 Calidad

El RGPD no menciona de forma expresa al principio de calidad, sino que constan descritos varios de sus elementos: exactitud y actualización. El artículo 5.1., literal d), señala que los datos personales deberán ser "exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»)".

Como antecedente de lo mencionado, consta en la sentencia ya indicada del caso Google Spain y Google, emitida el 13 de mayo de 2014 y resuelta por el Tribunal de Justicia de la Unión Europea, que "incumbe al responsable del tratamiento garantizar que los datos personales sean [...] exactos y cuando sea necesario actualizados", desplegando con ello la serie de características que componen una data de calidad.[699]

Entretanto, la normativa española señala en el artículo 4 de la LOPDGDD que, "conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados".

La exactitud[700] y veracidad[701] de los datos debe cuidarse en el momento de su recogida, pero fundamentalmente cuando son parte de las bases de datos de uso cotidiano. Ya que existirá un motivo de sanción si los datos no reflejan la "realidad actual"[702] de una persona.

---

[699] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, "Asunto C-131/12, en el caso: Google Spain y Google", 2014, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES.

[700] Son datos exactos aquellos que "guardan absoluta equivalencia con la información recibida antes de ser manipulada para su tratamiento". A. RUIZ CASTILLO, *Los datos de carácter personal* (Barcelona: Editorial Bosch, 1999), 41.

[701] "Es cierto todo dato demostrable, contrastable e identificable con una información que se halla fuera del ámbito en donde se encuentra el dato. La certeza se deriva de la exactitud; no de la veracidad o inveracidad de la información. Es cierto todo dato exacto, demostrable y contrastable con la información que ha dado lugar a su nacimiento. La información ha de tratarse objetivamente prescindiendo de la intención del que entrega la información que ha de convertirse en dato. Otra cosa será la responsabilidad objetiva civil o penal del que ofrece información inveraz que derive en dato falso". RUIZ CASTILLO, *Los datos de carácter personal*, 42.

[702] "En la antigua Ley se decía que debía responder, con veracidad, a la situación real del afectado, en la LOPD se ha cambiado esta palabra por la de actual. Según el Diccionario de la Real Academia española de la Lengua real significa que tiene existencia verdadera y efectiva, y actual que existe, sucede o se usa en el tiempo de que se habla. Parece que la palabra actual tiene un carácter más temporal". E. DEL PESO NAVARRO, *Ley de Protección de Datos*, 19. En el mismo sentido, la SAN recurso 602/2001, 31 de mayo de 2002; SAN recurso 711/2001, 6 de junio de 2002; SAN recurso 656/2001, 10 de mayo de 2002 y SAN recurso 798/2001, 7 de junio de 2002 dice: "el cambio interpretativo del artículo 4.3 y 28.3 por el actual 4.3 que reproduce el artículo 6 de la Directiva 95/46 del Parlamento Europeo y del Consejo de 24 de octubre – y 29.4 en concreto el cambio de la expresión 'situación real' por 'situación actual', implica que no se pueda mantener el saldo cero que este dato alude al pasado como deudor del afectado, y no a su estado actual en el que la deuda ha sido cancelada, que esta equiparado al de otros que no estuvieron nunca incluidos en u fichero de esta naturaleza. El artículo 29.4 introduce el adverbio 'siempre' respecto del reflejo veraz de una situación actual,

Por eso, el mayor problema que plantea este principio es la actualización de los datos que posibilite su veracidad y exactitud.

No obstante, el responsable del fichero "no podrá adivinar los cambios de los datos de los afectados. Pero sí podrá prevenirles en algún momento y anunciarles que cualquier cambio en sus datos debe ser comunicado por una vía establecida al efecto, que pueda ser el derecho de rectificación".[703] Esta prevención debe hacerse al afectado-cliente en tantos momentos como sean necesarios, ya que el vínculo no se limita a la temporalidad de un contrato, sino a la larga y continua relación que un responsable de tratamiento quiere establecer con los titulares de los datos.

Ahora bien, para que un responsable cumpla con el principio de calidad de datos, deben establecerse mecanismos que permitan demostrar su voluntad de cumplir su obligación de mantenerlos actualizados. Un mecanismo a implementarse es aquel que obliga al responsable del fichero a realizar "corrección de errores y la actualización de oficio, efectuando cambios necesarios para que los datos respondan a la situación actual del interesado".[704]

Otro mecanismo es permitir que los datos sean visibles a fin de posibilitar su verificación, mediante la consulta por parte de su titular. Sin embargo, esta consulta no es posible y por tanto exime de responsabilidad al responsable cuando:

> [...] los datos obtenidos de fuentes accesibles al público la LORTAD no exige la notificación del registro del afectado, difícilmente puede saber el titular del fichero si el dato obtenido de dichas fuentes es o no correcto y, además en el caso de autos, dado que en el Edicto no consta otro dato que el nombre y apellidos de los demandados, nunca hubiera sido posible efectuar tal notificación, ni averiguar la exactitud del dato publicado, ni de lo actuado puede afirmarse que dicho dato se refiere siquiera al denunciante, por lo que en la medida que no conste al titular del fichero la inexactitud del dato registrado, inexactitud que, reiteramos, no consta, no existe para éste obligación legal de cancelar el dato.[705]

El responsable del fichero está obligado a establecer procedimientos que garanticen que, una vez que se tenga conocimiento de la inexactitud de los datos, ya sea como una actitud de oficio o iniciada a petición de parte, se proceda inmediatamente a su modificación. Resulta fundamental, entonces, identificar desde cuando el responsable tiene conocimiento de la inexactitud de un dato, porque la ley obliga a mantener datos exactos y puestos al día, y "la palabra mantener denota una idea de permanencia temporal, por lo que, a juicio de esta Sala y Sección, la acción típica consistirá en la conservación de un dato no actualizado,

---

y sin duda alguna la situación actual del afectado es la de no tener ninguna deuda pendiente, y los que no tienen la condición de deudores no pueden reflejarse su saldo, ni siquiera como 'saldo 0'".

[703] D. SANTOS GARCÍA, *Nociones generales de la Ley Orgánica de Protección de Datos*, 57.

[704] C. ALMUZARA ALMAIDA, "Relaciones precontractuales y contractuales", 142.

[705] N. SÁNCHEZ MOURIS, "Los datos personales en el inicio de la actividad empresarial", en Directoras: A. MARZO PORTERA y F. RAMOS SUÁREZ, *La Protección de Datos en la Gestión de Empresas*, 55 y ss.

o, el mantenimiento de un dato erróneo una vez se tienen conocimiento de su inexactitud".[706]

Los principios de veracidad, exactitud y actualización también deben observarse cuando se sometan los datos a determinado tratamiento, a nuevas finalidades y a múltiples cesiones o comunicaciones.

Finalmente, el nivel de responsabilidad es mayor cuando los datos conforman parte de una base de datos común de solvencia patrimonial y crédito, pues la diligencia requerida obliga a "realizar barridas periódicas que aseguren la exactitud y actualidad"[707] de los datos, debido a que su inexactitud produce un alto riesgo respecto de la vulneración de otros derechos fundamentales (art. 20 LOPDGDD).

Por eso, posibles soluciones para garantizar la actualidad de los datos es la implementación de campañas de actualización de datos, o el aprovechamiento de la funcionalidad de los departamentos de servicio al cliente, posventas o de gestión de incidencias y la habilitación de un sistema ágil de comunicaciones interno y externo entre todos los canales y puntos de contacto.

Todo lo cual, además de facilitar el cumplimiento del principio de calidad de datos garantiza el derecho de acceso, rectificación y cancelación de los datos de los afectados; permite el adecuado planeamiento estratégico de los responsables, los cuales también necesitan que los datos que utilizan en sus modelos de negocio sean veraces, exactos y actuales.

Conforme lo analizado, el considerando 39 del RGPD señala que los responsables deben tomar todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos.

6.5.4.4 Finalidad

El principio de finalidad nace como respuesta a las acciones que responsables de tratamiento realizaron por muchos años, en el que usaron datos personales sin sentido de protección o cuidado, menos aún de prevención del daño a sus titulares, pues solo eran concebidos como activos digitales que debían ser usados en favor de la actividad o negocio.

> La autorregulación, a estas alturas, es deseable pero insuficiente. En el espacio que brinda la ausencia de reglas protectoras, han nacido prácticas con décadas de asentamiento, como la recolección de huellas dactilares o números de identidad para condicionar la entrega de

[706] STSJC, de 10 de mayo de 2000.
[707] N. SÁNCHEZ MOURIS, "Los datos personales en el inicio de la actividad empresarial", 49.

> servicios, la formación de bases de datos opacas, fugas de datos sin compensación alguna, y un constante desdén por la idea del consentimiento y la finalidad.[708]

De lo visto, a través del principio de finalidad se otorga sentido el almacenamiento y tratamiento de la información. Ya que, los responsables de tratamiento están obligados a dimensionar los objetivos para los cuales se obtuvieron y se procesarán los datos personales. Pero además, la identificación de la finalidad del tratamiento permite dimensionar riesgos, facilitar mecanismos de control y dotar de información suficiente para que el titular del dato pueda tomar una decisión sobre la entrega o no de su información.

Adicionalmente, se ha señalado respecto de finalidad y necesidad lo siguiente:

> Las que apuntan a la relación que debe existir entre el tratamiento informático de datos personales que se pretende y el cumplimiento de una finalidad legítima. Se trata de una relación de necesidad. Es decir, el tratamiento ha de ser necesario para lograr ese objetivo legítimo. Naturalmente, la desaparición de esa necesidad, elimina el presupuesto que ampara el tratamiento y dota, de este modo, de un carácter de temporalidad a la conservación y utilización de esta información. 2.a Las que se refieren a la adecuación que entre finalidad e información utilizada debe existir. Esta exigencia añade a la anterior el fundamental elemento de la proporción o medida: el tratamiento, además de necesario, ha de ser adecuado, es decir, razonable a la vista del fin que se pretende.[709]

En cuanto al principio de finalidad y su interrelación con los otros principios se ha dicho que:

> El principio de Finalidad se encuentra mencionado en los principios de pertinencia, consentimiento y propósitos legítimos y justos ya que debe verificarse la pertinencia y necesidad de los datos, de conformidad con los fines legítimos y justos por los cuales fue solicitado y que fuera autorizado previo consentimiento transparente y no podrán divulgarse ni ponerse a disposición para fines distintos.[710]

El RGPD en el artículo 5 sobre los principios relativos al tratamiento señala: "1. Los datos personales serán: [...] c) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo

---

[708] M. P. CANALES, J.C. LARA, "Lejos de proteger nuestros datos en américa latina", *@derechos digitales Derechos Humanos y Tecnologías en América Latina*, 3 de mayo de 2018, accedido el 15 de noviembre de 2019, https://www.derechosdigitales.org/12058/lejos-de-proteger-nuestros-datos-en-america-latina/

[709] P. L. MURILLO DE LA CUEVA, "La construcción del derecho a la autodeterminación informativa", *Revista de Estudios Políticos (Nueva Época)*, Núm. 104. Abril-Junio 1999, accedido el 11 de noviembre de2019, 52

[710] COMITÉ JURÍDICO INTERAMERICANO DE LA OEA, *Informe Privacidad y Protección de Datos Personales No. CJI/doc. 474/15 rev.2*, Rio de Janeiro, 26 de marzo de 2015, accedido el 2 de noviembre de 2019, http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_documentos_referencia_CJI-doc_474-15_rev2.pdf

en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»)".

El considerando 39 del RGPD señala que "las personas físicas deben tener conocimiento de [...] los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios".

De lo transcrito, se concluye que el principio de finalidad se relaciona directamente con el deber de información, puesto que el responsable debe informar especialmente respecto de los fines específicos del tratamiento de datos personales, que deben ser explícitos y legítimos y determinarse en el momento de la recogida. Esto debido a que, es indispensable esta determinación para realizar controles posteriores que puedan ayudar a identificar posibles transgresiones a otros derechos fundamentales, sobre todo aquellos casos de tratamientos que pudieran resultar discriminatorios o que pretendan una manipulación de la voluntad o la intromisión en la vida privada.

Además, el principio de finalidad es el elemento de base para determinar cuándo un dato es adecuado, pertinente o limitado en su uso, pues todo ello se mide en su relación con el fin declarado por el responsable del tratamiento, quien dependiendo de su modelo de funcionamiento o negocio determina con su voluntad el tratamiento que quiere realizar a los datos personales, y por ende es su responsabilidad que estos sean congruentes y respetuosos de las personas, así como éticos para con su propio giro organizacional como para con los titulares de los datos que se interrelacionan con él. De modo que la primera revisión es la de si la finalidad es legítima y lícita, y luego se puede examinar si el tratamiento es coherente o responde a la finalidad señalada, por tanto si es adecuado, pertinente y limitado.

El considerando (50) del RGPD determina que el tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales.

El principio de finalidad está directamente relacionado con la voluntad del responsable del tratamiento respecto de los usos y utilizaciones posteriores que desea aplicar a la información personal. Sin embargo, conforme señala el considerando (33) del RGPD: "Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la

investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida".

En la normativa española el principio de finalidad e incompatibilidad se desarrollaba en el numeral 2 del artículo 4 de la derogada LOPD, que textualmente dice: "2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos". La LORTAD, igualmente derogada por la LOPD, prohibía el uso de los datos para fines "distintos" de los que motivaron la captación; mientras que la LOPD utiliza la palabra "incompatible".

Sin embargo, la jurisprudencia[711] ha entendido que finalidad incompatible es aquella distinta para la que fueron originalmente recabados los datos: "la principal argumentación empleada por los defensores de esta teoría es que si el artículo 4.1 exige que los datos sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se han obtenido, resultaría absurdo que pudieran aplicarse a finalidades distintas, aun cuando fueran compatibles".[712]

Por lo tanto, todos los datos recogidos en el "cumplimiento de una relación laboral, negocial o administrativa, solo podrán ser usados en el estricto ámbito del contrato que los legitima para su uso. En este supuesto, utilizar los datos para otras finalidades supone la violación del principio de calidad de datos. Se requerirá en este caso concreto solicitar el consentimiento para realizar el tratamiento deseado, con arreglo al principio de calidad de datos".[713] Esta forma de limitación del uso de los datos personales para finalidades incompatibles para las que fueron recabados faculta el cumplimiento del principio de consentimiento, permitiendo que este "sea legítimo, cuando resulte exigible, o bien acortar los tratamientos lícitos de la información, cuando dicho consentimiento deba ser excluido, especialmente en los casos de los poderes públicos".[714]

---

[711] Las sentencias SAN recurso 119/2002, 11 de febrero de 2004 y SAN recurso 1067/2000, 8 de febrero de 2002, clarifica lo señalado pues sostienen que "la nueva redacción, recogida en el artículo 4.2 de la LOPD no puede tener un sentido distinto del que ese mismo precepto de la LORTAD imponía. Razonó la Audiencia Nacional que en castellano la palabra incompatible entraña repugnancia entre dos cosas o términos y que si se pretendiera limitar esta cláusula solamente a los supuestos en que se diera esa contradicción, eso equivaldría a dejarla sin efecto porque en muy pocos supuestos existiría una contradicción de tal naturaleza. Por eso, llegó a la conclusión que por fines incompatibles había que entender fines distintos, ya que, además, esa solución era la que mejor se ajustaba a los principios de la ley y a la relevancia que atribuye al consentimiento que, interpretando el artículo. 6.2, entiende necesario cuando se pretenda usar esos datos para finalidades diferentes de las iniciales. Línea está en la que también se encuentran STSJCV 1901/2002, de 27 de noviembre y la STSJCM 90/2003, de 29 de enero".

[712] En el mismo sentido, las sentencias dictadas por la STSJCM, 7 de diciembre, la STSJCM, 15 de noviembre, la STSJCM, 12 de julio y la STSJCM, 25 de enero del 2000.

[713] D. SANTOS GARCÍA, *Nociones generales de la Ley Orgánica de Protección de Datos, cit.,54.*

[714] J. PIÑAR MAÑAS, coord., "Estrategias de la Red Iberoamericana de Protección de Datos", *Red Iberoamericana de Protección de Datos, Declaraciones y Documentos* (Valencia: Tirant lo Blanch, 2006), 69.

Además, este principio también se relaciona directamente con el de información, ya que el responsable del fichero deberá comunicar al afectado de todos los aspectos que involucra la recogida de datos, y que evidentemente incluye la finalidad o finalidades del fichero y los posibles tratamientos a los que serán sometidos sus datos. En este sentido, el vigente artículo 11 LOPDGGD determina que el responsable del tratamiento debe informar al afectado en todo caso de "la finalidad del tratamiento".

Finalmente, siempre se ha venido reconociendo una excepción al principio de incompatibilidad que se produce cuando el tratamiento posterior de los datos se refiere a fines históricos, científicos o estadísticos, los cuales para su utilización deben estar disociados (art. 5.1 e) RGPD).

La Agencia Española de Protección de Datos en su Memoria correspondiente al ejercicio 2000, respecto del alcance de los términos "datos históricos" ha señalado:

> Para delimitar qué ha de entenderse como datos históricos, debe recordarse que el artículo 57.1 c) de la Ley 16/1985, de 25 de junio, reguladora del Patrimonio Histórico Español establece que «los documentos que contengan datos personales de carácter policial, procesal, clínico, o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de 25 años desde su muerte si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos».

Si bien la LOPD señalaba que no existía incompatibilidad de la finalidad de los ficheros cuando se usen para fines históricos, sin embargo, de la posición de la AEPD citada, la única forma en la que podrían llegar a utilizarse, sin autorización previa y expresa de sus titulares, es cuando tengan una antigüedad mayor de 25 años si se conoce de la fecha del fallecimiento de su titular y de 50 años contados desde la fecha de los documentos, si se desconoce la fecha del fallecimiento y, además, cuando se encuentren debidamente disociados (*vid.*, art. 26 LOPDGDD).

En consecuencia, los datos necesarios para realizar investigaciones de mercado, estudios de industrias, de grupos objetivos, que se necesita para la elaboración inicial de varios modelos de segmentación y que se configuran mediante datos históricos y estadísticos de mercados, productividad, oferta y demanda, etc. deberán contar con autorización previa de sus titulares, estar apropiadamente disociados o tener la antigüedad señalada de 25 y 50 años conforme se señaló oportunamente, que los califica de datos históricos.

Por su parte, el artículo 6 del RGPD, referente a la licitud del tratamiento, señala en el numeral 4 que cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o la ley

debe constituir una medida necesaria y proporcional en una sociedad democrática para salvaguardar: a) la seguridad del Estado; b) la defensa; y c) la seguridad pública.

En otras palabras, que no se autoricen tratamientos o cesiones o cambio de finalidad, sino únicamente cuando sean compatibles con el fin para el cual se recogieron inicialmente. Para lo cual, los criterios que otorgan proporcionalidad son los previstos en el artículo 6.4 del RGPD que hacen referencia a: "a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto; b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento; c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10; d) las posibles consecuencias para los interesados del tratamiento ulterior previsto; e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización".

6.5.4.5 Seguridad adecuada al riesgo

A la seguridad, tradicionalmente se la concibe como principio de protección de datos personales. Pero su aplicación no debe estar sesgada a temas de implementación de infraestructuras tecnológicas sino que conforme señala el Informe sobre la economía digital 2019: creación y captura de valor: repercusiones para los países en desarrollo dictada por la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, UNCTAD se determina que:

> La privacidad y la seguridad de los datos requieren una atención especial. Es importante adoptar medidas de seguridad para proteger a la sociedad contra el uso indebido de los datos de forma deliberada. Se necesitan leyes y reglamentos para combatir el robo de datos personales; para establecer normas sobre qué datos personales pueden recopilarse, utilizarse, transferirse o eliminarse y cómo puede hacerse; y para garantizar que los modelos empresariales basados en los datos generen beneficios para el conjunto de la sociedad.[715]

Por su parte, el artículo 5, literal f), del RGPD señala que "los datos personales serán tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)".

[715] ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Informe sobre la economía digital 2019: creación y captura de valor: repercusiones para los países en desarrollo,* 04 de septiembre de 2019, accedido el 11 de noviembre de 2019.

En ese sentido, el artículo 4, numeral 12, del RGPD establece un concepto sobre "violación de la seguridad de los datos personales", que coincide literalmente con la cita antedicha y que establece que debe ser entendida como toda violación de la seguridad que ocasione al menos una de las siguientes consecuencias:

i. la destrucción de datos personales;
ii. pérdida de datos personales;
iii. alteración accidental de datos personales;
iv. alteración ilícita de datos personales;
v. transmitidos, conservados o tratados de otra forma;
vi. la comunicación o acceso no autorizados a dichos datos.

Ahora bien, por la importancia del tema, la sección 2 del RGDP, denominada seguridad de los datos personales, contempla en los artículos del 32 al 34 el régimen que garantice la seguridad de estos datos, de tal manera que no solo es un principio, una definición y una obligación del responsable y del encargado, sino un sistema organizado, estratificado, estructurado e integral que debe ser previsto desde sus distintos enfoques para que pueda ser efectivo. En este sentido, a continuación se desarrolla lo siguiente:

i. Tipos de daños que pueden producirse de no tomarse medidas adecuadas oportunas

El considerando (85) señala que si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como:

a) pérdida de control sobre sus datos personales;
b) restricción de sus derechos;
c) discriminación;
d) usurpación de identidad;
e) pérdidas financieras;
f) reversión no autorizada de la seudonimización;
g) daño para la reputación;
h) pérdida de confidencialidad de datos sujetos al secreto profesional
i) cualquier otro perjuicio económico o social significativo para la persona.

ii. Condiciones que deben tomarse en cuenta para establecer un nivel de seguridad adecuado al riesgo

El artículo 32 del RGPD establece que para garantizar un nivel de seguridad adecuado al riesgo que se deriva del tratamiento de los datos personales, se deberá tomar en cuenta:

a) el estado de la técnica;
b) los costes de aplicación;

c) la naturaleza, el alcance, el contexto y los fines del tratamiento;
d) los riesgos de probabilidad que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;
e) la gravedad de las variables para los derechos y libertades de las personas físicas;
f) "la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales" (considerando (83), RGPD).

iii. Medidas para mitigar y garantizar un nivel de seguridad adecuado al riesgo

Antecedente de la concepción actual de medidas para mitigar y garantizar un nivel de seguridad adecuado al riesgo que ahora se encuentra recogido en el RGPD consta en la sentencia del caso Worten, emitida el 30 de mayo de 2013 y resuelta por el Tribunal de Justicia de la Unión Europea sobre la obligación del Estado portugués de prever medidas técnicas y organizacionales para la protección de datos, atendiendo al artículo 17 de la Directiva 95/46 que señala: "los Estados miembros deben establecer la obligación del responsable del tratamiento de los datos personales de aplicar las medidas técnicas y de organización destinadas a garantizar un nivel de seguridad adecuado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse".[716]

El considerando (83) y el citado artículo 32 del RGPD señalan que el responsable y el encargado del tratamiento deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, para garantizar un nivel de seguridad adecuado al riesgo y evitar infringir el Reglamento. Estos mecanismos deben tomar en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse y consistirán en:

a) Medidas técnicas apropiadas.
b) Medidas organizativas apropiadas.
c) La seudonimización.
d) El cifrado de datos personales.
e) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

[716] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-342/12, en el caso: Worten], 2013, accedido 13 de octubre de 2018, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62012CJ0342

f) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
g) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
h) La adhesión a un código de conducta aprobado a tenor del artículo 40, podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.
i) La obtención de un mecanismo de certificación aprobado a tenor del artículo 42, podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.
j) El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

iv. Sobre el formato y los procedimientos aplicables a la notificación de las violaciones de la seguridad de los datos personales

De conformidad con el considerando (88) del RGPD, relativo a las disposiciones de aplicación sobre el formato y los procedimientos aplicables a la notificación de las violaciones de la seguridad de los datos personales, se deberán seguir los siguientes criterios:

a) Debe tomarse en cuenta las circunstancias de la violación de seguridad de los datos personales, inclusive si los datos personales habían sido protegidos mediante las medidas técnicas de protección adecuadas, limitando eficazmente la probabilidad de usurpación de identidad u otras formas de uso indebido.
b) El responsable del tratamiento comunicará tal violación al interesado sin dilación indebida, esto es que deben realizarse "tan pronto como sea razonablemente posible".
c) Deberá realizarse en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales.
d) Debe tomarse en cuenta los intereses legítimos de las autoridades policiales, ya que en caso de que una comunicación prematura pueda obstaculizar innecesariamente la investigación de las circunstancias de una violación de la seguridad de los datos personales.
e) Una rápida comunicación se puede justificar, por ejemplo, ante la necesidad de mitigar un riesgo de daños y perjuicios inmediatos (considerando (86), RGPD).
f) Una comunicación que lleve más tiempo se justifica por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares (considerando (86), RGPD).

v. Obligaciones, notificación y comunicación en caso de violaciones a la seguridad de los datos personales

El artículo 33 establece que en caso de violación de la seguridad de los datos personales, se deberá:

a) Notificación a la autoridad de control

   a. Al tenor del considerando (84) y del artículo citado del RGPD, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales se deberá notificar a la autoridad de control competente, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que, que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.
   b. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

b) Notificación del encargado del tratamiento al responsable de tratamiento

   El encargado de tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

c) Comunicación al interesado

   El considerando (86) y el artículo 34 del RGPD determinan la obligación de comunicar una violación de la seguridad de los datos personales al interesado, cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, y permitirle tomar las precauciones necesarias.

   La comunicación de violación de seguridad de los datos personales al interesado deberá cumplir con lo siguiente:

   a. Debe describir la naturaleza de la violación de la seguridad de los datos personales.

b. Las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.
c. Se describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales.
d. Contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, literales b), c) y d).
e. No será necesaria la comunicación si se cumple alguna de las condiciones siguientes:

i. el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
ii. el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concrete el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;
iii. suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados;
iv. cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

d) Facilitar información simultánea.

Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

e) Documentar cualquier violación.
f) El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

vi. Contenido mínimo de las notificaciones sobre violaciones de seguridad de los datos personales

Acorde a lo dispuesto en el artículo 33 del RGPD, el contenido mínimo de la notificación sobre violaciones de seguridad de los datos personales deberá:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

vii. Verificaciones que permiten determinar la violación de la seguridad de los datos personales

Al tenor del considerando (87) del RGPD, para determinar la violación de la seguridad de los datos personales debe:

a) verificarse si se ha aplicado toda la protección tecnológica adecuada;
b) si se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales;
c) si se han tomado las medidas organizativas oportunas para informar sin dilación a la autoridad de control;
d) si se han tomado las medidas organizativas oportunas para informar sin dilación al interesado;
e) verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado;
f) dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el Reglamento.

6.5.4.6 Consentimiento

Conforme el contenido del artículo 4, numeral 11) del RGPD se entiende por consentimiento del interesado "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

El principio del consentimiento es la piedra angular del sistema de protección de datos personales, pues por su intermedio el titular de los datos puede ejercer el derecho a la libertad informática, es decir, a controlar su datos y decidir qué y a quiénes, en qué condiciones y con qué finalidades entregarlos. En efecto, el consentimiento es mecanismo que garantiza el derecho a la autodeterminación informativa. Solo mediante el consentimiento expreso, inequívoco e informado, el responsable del tratamiento puede captar, tratar y ceder datos personales.

El considerando (32) del reglamento europeo señala que "el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta."

Es decir, el consentimiento es uno de los principios más importantes de la protección de datos personales; es la manifestación de voluntad libre de vicios que acepta de forma informada sobre la recogida y tratamiento de sus datos personales. Esta aceptación debe ser entendida como una declaración o una acción afirmativa; esto quiere decir, desde la teoría de los actos jurídicos, que debe exteriorizarse la voluntad y por ende no es posible la aceptación tácita, puesto que la diferencia entre la manifestación y la declaración es precisamente el elemento de demostración por la cual existe una materialización verbal, física como la de hacer un clic.

Desde la perspectiva de la normativa europea, solo es consentimiento aquel que reúne los siguientes requisitos: libre, específico, informado e inequívoco, pues solo si se cumple con estos supuestos indispensables, se puede hablar de consentimiento válido. A continuación, se analizará cada uno de estos requisitos.

a) Libre. Se entiende aquel que ha sido obtenido libre de los vicios del consentimiento que establece el Código Civil;[717] es decir, sin inducir a error, sin utilizar la fuerza o la intimidación y

[717] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Memoria de la Agencia Española de Protección de Datos correspondiente al ejercicio 2000*, accedido 16 de junio dl 2007, en https://www.agpd.es/upload%2FCanal_Documentacion%2FInformes%20Juridicos%2FConsentimiento%2FC

sin que medie dolo. En otras palabras, obliga a las empresas a actuar con absoluta lealtad al cliente no solo en el cumplimiento de los principios de información, legalidad y calidad de datos, sino principalmente porque de no cumplirse el consentimiento sería inválido y no facultaría la recogida, tratamiento e inclusión en una base de datos.

El considerando (43) del RGPD señala que "para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento". Es decir, se protege a las personas titulares de los datos, que en una relación de poder relacionada con desequilibrios debido a la fuerza coercitiva del Estado, o desde la perspectiva de una relación negocio y consumidor pudiera ser perjudicada la persona natural que por acceder a bienes o servicios y beneficios sociales se encuentra en estado de desventaja y se encuentra forzada, directa o indirectamente, a ceder sobre su autodeterminación informativa.

b) Específico. Es aquel que permite al interesado un conocimiento definido, determinado y concreto de la operación, del tratamiento y de las finalidades explícitas, sobre todo respecto de datos sensibles, conforme el artículo 9.2, literal a) del RGPD; decisiones individuales automatizadas, incluida la elaboración de perfiles (art. 22, RGPD); flujo trasfronterizo de datos personales (art. 49, RGPD). De la recolección de sus datos y de su inclusión en una base de datos, no caben interpretaciones extensivas o analógicas, ya que no sería procedente establecer un consentimiento continuado para futuros tratamientos ni para una cesión indefinida.

Una clara necesidad del requisito de especificidad para la configuración del consentimiento lo hace, dentro de los Planes de Oficio 2002, al sector de la Banca a Distancia que dicta el Consejo Consultivo cuando señala que: "ha detectado la práctica de incluir cláusulas que informan de forma genérica sobre cesiones a empresas del grupo para la oferta y contratación de otros productos y servicios sin que se concrete con mayor detalle la información aportadas y sin que se recoja en el propio contrato ningún procedimiento que permita expresar dicha oposición, como por ejemplo la inclusión de una casilla al efecto"[718].

El requisito de especificidad se relaciona directamente tanto con el deber de información como con el de calidad de datos, acerca de la finalidad e incompatibilidad de los datos porque "la determinación de las finalidades debe ser lo más concreta posible y deberá abarcar los usos

---

OM%20%282000-0000%29%20%28caracteres%20del%20consentimiento%20definido%20por%20la%20LOPD%29.pdf

[718] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Memoria 2002*, accedido el 15 de noviembre de 2019, https://www.aepd.es/media/memorias/memoria-AEPD-2002.pdf

actuales y los que se pretendan realizar por parte del responsable del tratamiento. Debe así tenerse en cuenta que la concreción de la finalidad limita la actuación del responsable frente a futuros tratamientos".[719]

En consecuencia, se debe especificar detenidamente todos y cada uno de los procesos o tratamientos actuales y futuros, a los que se van a someter los datos del titular, a fin de recabar su consentimiento, que en definitiva autorice al responsable del fichero a realizar dichos tratamientos y le evite sanciones por el cometimiento de una infracción considerada como grave (art. 44.3, literal c), LOPD), como es la de realizar tratamientos de los datos de carácter personal sin el consentimiento específico del interesado.

c) Informado. El consentimiento guarda estrecha relación con el principio de información, ya que depende de él para su existencia. Si es que el deber de información ha sido realizado de forma correcta (información del tratamiento de los datos, de forma expresa, precisa e inequívoca) y completa (de acuerdo con los deberes y excepciones que constan en el RGPD); se puede concluir que el consentimiento otorgado por el titular de los datos ha sido informado.

d) Inequívoco. La normativa española recogía el término inequívoco en lugar de explícito, pero le atribuía el mismo significado, ya que "cuando no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento".[720] Resulta sencillo considerar como consentimiento inequívoco al expreso o al explícito, porque es una manifestación exteriorizada de la voluntad.

El RGPD resuelve una vieja discusión por la que se acepta únicamente al consentimiento inequívoco, expreso o explícito, mientras que el consentimiento tácito, es decir aquel que se "deriva de la inactividad, silencio o falta de oposición del afectado"[721] ya no es procedente. Varios autores sostenían que este consentimiento tácito era válido porque "para que se configure el consentimiento no se necesita que sea expreso para que sea inequívoco".[722] Incluso la misma Agencia Española de Protección de Datos en la "Memoria" correspondiente al ejercicio 2000 establecía que: "de las características del consentimiento no se infiere necesariamente su carácter expreso en todo caso, razón por la cual aquellos supuestos en los que el legislador ha supuesto que el consentimiento deba revestir ese carácter, lo ha indicado expresamente; así sucede en el caso del tratamiento de datos especialmente protegidos indicando el artículo 7.2 la necesidad de consentimiento expreso y escrito para el tratamiento de los datos de ideología, religión, creencias y afiliación sindical y, el artículo 7.3, la necesidad de consentimiento expreso aunque no necesariamente escrito para el tratamiento de los datos relacionados con la salud el origen racial y la vida sexual. Por tanto, el consentimiento

[719] C. ALMUZARA ALMAIDA, "Relaciones Precontractuales y contractuales", *Estudio Práctico sobre la Protección de Datos de Carácter Personal*, 101.
[720] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Memoria de la Agencia Española de Protección de Datos correspondiente al ejercicio 2000*, ibíd.
[721] N. SÁNCHEZ MOURIS, "Los datos personales en el inicio de la actividad empresarial", 68.
[722] SÁNCHEZ MOURIS, "Los datos personales en el inicio de la actividad empresarial",. 66-7; DEL PESO NAVARRO, *Ley de Protección de Datos*, 21; y DAVARA RODRÍGUEZ, *Manual de Derecho Informático*, 88.

anteriormente podía ser tácito, en todo tipo de datos, incluso en el tratamiento de datos que no sean especialmente protegidos (arts. 7.2 y 7.3, LOPD), a tal punto que sugería otorgar al interesado un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento del mismo".

En términos parecidos se ha pronunciado la SAN recurso 619/2002, 30 de junio de 2004, y en el mismo sentido también la STS recurso 7707/2000, 18 de marzo de 2005: que se podía probar que el interesado había recibido la información como certificación de la carta, acuse de recibo, reporte electrónico sobre la apertura y revisión del e-mail, siempre y cuando dichos documentos reúnan los requisitos mínimos;[723] si no había oposición se entendía consentimiento tácito.

Todas estas consideraciones han sido superadas y bajo los nuevos estándares europeos que fortalecen la protección de datos personales, ya no se permite el consentimiento tácito como equiparable a consentimiento explícito. Por eso consta en el citado artículo 4, numeral 11 del RGPD, la frase "una declaración o una clara acción afirmativa", por la cual se determina que solo el consentimiento expreso se considerará válido para un adecuado tratamiento.

Ahora bien, en la Guía del RGPD para responsables de tratamiento se señala que "el consentimiento puede ser inequívoco y otorgarse de forma implícita cuando se deduzca de una acción del interesado (por ejemplo, cuando el interesado continúa navegando por una web y acepta así el que se utilicen cookies para monitorizar su navegación)";[724] de esta manera no resulta en una inacción como ocurría con el consentimiento tácito, sino que se entiende que existe una acción implícita como la de continuar navegando.

Cabe anotar que para datos especiales, conforme el considerando (51) del RGPD, amerita un nivel de protección reforzado, por su naturaleza "particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales", de tal forma que los datos deben ser tratados, en situaciones específicas contempladas en el RGPDR, además conforme lo que cada Estado miembros establezca en su normativa interna, sobre todo, en lo que se refiere a las condiciones de licitud del tratamiento; esto debido a que la norma ahora establece una prohibición general de tratamiento a menos que se cumplan las condiciones establecidas expresamente en el RGPD, conforme consta en el artículo 9 del citado cuerpo legal.

[723] Así fue sancionada una empresa por no poder acreditar la efectiva recepción de la carta por el interesado dada la falta de rigor con la que fue realizado el certificado por la empresa distribuidora". Ver Memoria de la Agencia Española de Protección de Datos correspondiente al ejercicio 2002.

[724] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, AGENCIA CATALANA DE PROTECCIÓN DE DATOS, Y AGENCIA VASCA DE PROTECCIÓN DE DATOS, *Guía del Reglamento General de Protección de Datos para responsables de tratamiento*, accedido 14 de octubre de 2018, https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf.

En consecuencia, se requiere de consentimiento inequívoco y explícito para el tratamiento de datos sensibles, la adopción de decisiones automatizadas y las transferencias internacionales, conforme el artículo 9.2 a.[725]

e) El momento de la recogida del consentimiento. A diferencia del principio de información, no existe limitación temporal en la recogida del consentimiento, por lo tanto puede ser previa o posterior al tratamiento, aunque no en todos los casos, pues cuando se necesite consentimiento expreso, debe realizarse previamente debido a la protección especial que revisten, por ejemplo, los datos sensibles. Se puede tratar datos sensibles cuando el interesado otorga su consentimiento explícito, excepto si la normativa de cada Estado miembro establece expresamente que el titular no puede autorizar el tratamiento de este tipo de datos (art. 9, lit. a), RGPD).

El artículo 7 del RGPD señala las condiciones para que se reconozca la validez del consentimiento las siguientes:

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del Reglamento"

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

El considerando (42) del RGPD señala que "de acuerdo con la Directiva 93/13/CEE del Consejo, debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno".

[725] *Ibíd*.

En lo que respecta al consentimiento, el Tribunal de Justicia de la Unión Europea ya asentó precedentes de excepción, así por ejemplo, la sentencia del caso Tele 2, emitida el 15 de marzo de 2017, con respecto al consentimiento de los abonados y la publicación de sus datos personales en guías en función al artículo 5, apartado 2 de la Directiva, declara que "no es preciso que la empresa que asigna números de teléfono a sus abonados, formule la solicitud de consentimiento dirigida al abonado de forma que éste exprese ese consentimiento de forma diferenciada en función del estado miembro al que dichos datos pueden ser transmitidos". Allí se interpretó con anterioridad de manera errónea el artículo antes indicado al mencionar que "tiene la obligación, con arreglo a la normativa nacional, de obtener el consentimiento [...] de forma diferenciada", a lo que el tribunal contestó que la interpretación adecuada se basa exactamente en la oposición a dicho enunciado.[726]

Respecto del consentimiento de los niños, el RGPD determina en el artículo 8 las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información:

> 1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.
>
> Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.
>
> 2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.
>
> 3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

En España, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ha establecido finalmente que el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años (tal y como se determinaba anteriormente), exceptuándose los casos en que se exija por ley la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento. En caso de menores de catorce años, el tratamiento de sus datos fundado en el consentimiento solo será lícito si

[726] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-536/15, en el caso: Tele 2", 2017], accedido 13 de octubre de 2018, http://blog.uclm.es/cesco/files/2017/03/STJUE-15-MARZO-2017-GUIA-TELEFONICA-CESCO.pdf

consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

El desarrollo de fenómenos como el big data, el internet de las cosas, la decisión algorítmica, el aprendizaje automático o la inteligencia artificial ponen en jaque elementos fundantes del sistema de protección de datos, tal como la noción de consentimiento. De tal suerte, surgen figuras como la del « interés legítimo » o la del « uso compatible de datos» que habilitan facultades de tratamiento más allá del conocimiento y consentimiento de su titular. La adopción de decisiones automatizadas y la elaboración de perfiles mediante algoritmos que pocos conocen o entienden excluyen, paradójicamente, a su protagonista principal. [727]

6.5.4.7 Principio de proporcionalidad

El considerando (4) del RGPD señala que "el tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística".

De lo transcrito se colige que el RGPD establece el principio de proporcionalidad desde dos enfoques: a) El primero, relativo al derecho a la protección de datos personales y otros derechos fundamentales; de tal forma que en caso de conflicto de derechos es indispensable realizar un ejercicio de ponderación, en el cual la proporcionalidad permita determinar los límites del derecho a la protección de los datos personales sobre todo en su función social y de equilibrio con otros derechos. b) El segundo, respecto de la proporcionalidad entre la protección de los datos de los titulares y el libre flujo informacional, es decir el respeto por la dignidad humana; al mismo tiempo que permitir el desarrollo económico, social y cultural que los avances tecnológicos plantean.

De otro lado, se puede comprender al principio de proporcionalidad al tenor de lo señalado en la sentencia del caso *Lindqvist*, emitida el 6 de noviembre de 2003 y resuelta por el Tribunal de Justicia de la Unión Europea, que menciona que:

[727] V. MILANÉS, *Op. cit. Cit.*

> […] si bien es cierto que la tutela de la intimidad requiere aplicar sanciones eficaces a las personas que efectúen tratamientos de datos personales sin atenerse a lo dispuesto en la Directiva 95/46, tales sanciones deben respetar en todo caso el principio de proporcionalidad", dejando como precedente que para el Tribunal el principio de proporcionalidad tiene que ver directamente con la aplicación de sanciones lo cual se aleja de la concepción tradicional que atañe el uso de este principio a su estricta relación con la finalidad del tratamiento.[728]

Como se desprende del texto transcrito, tradicionalmente el principio de proporcionalidad se encuentra asociado al principio de finalidad, de tal manera que:

> […] a) Hasta ahora se ha reconocido que la recolección coercitiva de datos sobre la persona no es procedente en forma ilimitada, principalmente cuando se trata de datos que van a ser utilizados por la administración (por ejemplo, para asuntos fiscales o para el otorgamiento de prestaciones sociales). Señalar hasta dónde el derecho a la autodeterminación de la información y, en relación con éste, el principio de proporcionalidad y la obligación de adoptar medidas de carácter procesal obligan al legislador –desde el punto de vista constitucional– a reglamentar este tipo de medidas, depende del tipo, extensión y posible utilización de los datos recolectados, así como del peligro de que se haga abuso de ellos (cf. BVerfGE 49, 89 [142]; 53, 30 [61]). Por lo general podrá considerarse la existencia de un interés general preponderante únicamente tratándose de datos con un contenido social, con exclusión de aquellas informaciones de carácter íntimo o que impliquen una autoincriminación, las cuales no pueden ser exigidas. Con base en el conocimiento y experiencia con que se cuenta hasta ahora, cobran particular relevancia. Para obligar a una persona a proporcionar datos personales es necesario que el legislador haya determinado en forma precisa y específica su finalidad y que las informaciones sean necesarias y adecuadas para el logro de dicha finalidad. De ahí que la recolección de datos en forma no anónima, acopiados con finalidades indeterminadas o no determinables, sea inadmisible. Todas las dependencias, que para el cumplimiento de sus funciones recojan datos personales, deberán también restringirse al mínimo requerido para alcanzar los fines que persiguen. [729]

Del texto transcrito, se desprende que el principio de proporcionalidad también guarda relación directa con el de minimización y pertinencia, dado que solo se podrá recabar aquellos datos que no sobrepasen la finalidad, apegados a una necesidad de recopilación para satisfacción del objetivo previamente acordado de recopilación de la información.

---

[728] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-101/01, en el caso: Lindqvist], 2003.

[729] Alemania: TRIBUNAL CONSTITUCIONAL FEDERAL, "Sentencia de la Primera Sala, del 15 de diciembre, 1983, BVerfGE 65, 1 [Censo de Población]", *Jurisprudencia del tribunal constitucional federal alemán: Extractos de las sentencias más relevantes compiladas por Jürgen Schwabe,* Compilador: R. HUBER (Fundación Konrad Adenauer, A.C.: México, 2009), 98.

Finalmente, el artículo 9 del RGPD señala el tratamiento de categorías especiales de datos personales, por las cuales se prohíbe el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física, a menos que el tratamiento sea necesario por razones de un interés público esencial, establecido en la ley, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

La proporcionalidad en este caso es uno de los requisitos necesarios para que sea posible el tratamiento de datos sensibles relacionados con un interés público. Como se ve, las condiciones son concurrentes por lo que se requiere todos y cada uno de estos para que se pueda garantizar proporcionalidad en el tratamiento de datos sensibles.

6.5.4.8 Principio de licitud

Conforme el considerando (39) del RGPD, "todo tratamiento de datos personales debe ser lícito y leal". Al respecto, consta como antecedente la sentencia del caso Google Spain y Google, emitida el 13 de mayo de 2014 y resuelta por el Tribunal de Justicia de la Unión Europea. Allí se expone que "incumbe al responsable del tratamiento garantizar que los datos personales sean tratados de manera leal y lícita"; en el mismo contexto expone los criterios que configuran el principio de calidad y el de conservación.[730]

En lo que incumbe al RGPD, este concibe un régimen más organizado de tratamiento de datos, pues propone el principio de licitud como base del sistema y ya no como se estilaba en legislaciones como la española en la que aparecían varias formas de tratamiento basadas en la sola autorización legal y en excepciones al consentimiento (art. 6, Ley Orgánica 15/1999 de España).[731] Es decir, constaban expresamente formulados en la ley los casos en los que era posible el tratamiento de datos personales sin la autorización del titular y a tales situaciones se determinaba como licitud. Ahora bien, el sistema ha cambiado y prima la legalidad, por la cual una de las formas autorizadas por la ley para el tratamiento es el consentimiento; además, existen otros mecanismos reconocidos como lícitos y siendo suficiente que uno de estos exista. Cabe agregar que ya no existe confusión tampoco con los ámbitos de aplicación y de inaplicación de la ley que están regulados expresamente en el artículo 2 del RGPD.

[730] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, "Asunto C-131/12, en el caso: Google Spain y Google", 2014, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES.

[731] España: *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*, 13 de diciembre de 1999, BOE 298, 14 de diciembre de 1999, 43088 a 43099 (12 págs.).

A continuación se hará referencia al contenido íntegro del artículo 6 del RGPD que establece las condiciones que debe cumplir el tratamiento para considerarse lícito. Tal como señala el considerando (40) del RGPD, para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida en propio RGPD o en la normativa de cada país, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato.

El artículo 6 se denomina "Licitud del tratamiento" y establece que el tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) *Consentimiento:* El interesado otorgue su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

b) *Ejecución de un contrato:* El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. Tal como señala el considerando (44) del RGPD, el tratamiento debe ser lícito cuando sea necesario en el contexto de un contrato o de la intención de concluir un contrato.

c) *Cumplimiento de una obligación legal*: El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. La ley debe desarrollar una normativa precisa que establezca la existencia de esta obligación legal y de los requisitos específicos del tratamiento y de otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento, conforme el artículo 6 numeral 2 RGPD y el considerando (45). Adicionando que, conforme señala esta misma norma, la base jurídica del tratamiento también debe constar expresamente en la ley, numeral 3; es decir, debe incluirse la finalidad del tratamiento, pero no se requiere que cada tratamiento individual se rija por una norma específica, sino que una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento

d) *Proteger intereses vitales:* El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física. "El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos

importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano (considerando [46], RGDP).

e) *Interés público o ejercicio de poderes públicos:* El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Nuevamente, en este caso, la ley debe recoger los casos de interés público o ejercicio de poderes públicos de forma expresa y además establecer los requisitos específicos del tratamiento y de otras medidas que garanticen un tratamiento lícito y equitativo, conforme el artículo 6 numeral 2, RGPD. Se agrega que, conforme señala esta misma norma, la base del tratamiento también debe constar expresamente en la ley, numeral 3, y en el considerando (45); es decir, debe incluirse la finalidad del tratamiento, pero no se requiere que cada tratamiento individual se rija por una norma específica, sino que una norma puede ser suficiente como base para varias operaciones de tratamiento de datos necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos.

   Además, podrá contener disposiciones específicas como "las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito, equitativo" y leal, incluido la determinación de la autoridad pública, persona jurídica o física de derecho público que sea considerada como responsable del tratamiento que realice la misión de interés público o el ejercicio de poderes públicos, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, o de derecho privado, como una asociación profesional; así como las relativas a otras situaciones específicas de tratamiento, al tenor del capítulo IX, artículo 6, numeral 3, literales a) y b) y parágrafo siguiente, y el considerando (45).

El considerando (52) del RGPD señala otras categorías de datos relativas al ámbito de la legislación laboral, de la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud, fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos, el ejercicio o la defensa de reclamaciones judiciales o administrativo o extrajudicial; para las cuales se debe establecer excepciones expresamente señaladas en la ley, de tal forma que, su tratamiento resulte lícito cuando sea en interés público y que además establezca medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas (considerando [54], RGPD).

El considerando (54), además aclara que se debe entender que el tratamiento de salud razones de interés público no debe dar lugar a tratar datos personales con otros fines a terceros, como empresarios, compañías de seguros o entidades bancarias.

El considerando (55) del RGPD menciona qué debe entenderse por razones de interés público también el tratamiento de datos personales realizado por las asociaciones religiosas reconocidas oficialmente.

En el mismo sentido, el considerando (56) del RGPD señala que será de interés público, y por tanto autorizado, el tratamiento de datos personales cuya finalidad sean actividades electorales realizadas por el Estado y por los partidos políticos, incluidas las opiniones políticas, siempre que se ofrezcan garantías adecuadas.

El artículo cincuenta y ocho bis de la Ley Orgánica 6/1985, de 19 de junio, del Régimen Electoral General española (introducido por la LOPDGDD), denominado "Utilización de medios tecnológicos y datos personales en las actividades electorales", estableció al respecto lo siguiente:

> 1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas. 2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.

No obstante, el Tribunal Constitucional, en su sentencia de 22 de mayo de 2019, lo declaró inconstitucional por vulnerar el "contenido esencial" del derecho fundamental a la protección de datos así como por la inexistencia de "garantías adecuadas".

f) *Satisfacción de intereses legítimos:* El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

En el considerando (47) se aclara que el interés legítimo "de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable". Ejemplos privados como señala el citado considerando es la relación pertinente y apropiada entre cliente y servicio del responsable.

> […] En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo (considerando [47], RGPD).

Otro grupo que manifiestamente tiene interés legítimo, al tenor del considerando (48), es el responsable que forma parte de un grupo empresarial o de entidades afiliadas a un organismo central dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados. Sobre esta temática es un concepto muy abstracto y que pudiera resultar incluso ambiguo determinar interés legítimo para el sector privado; más preciso puede ser la licitud o ilicitud del tratamiento determinado en la ley, de tal forma que las relaciones contractuales o las obligaciones legales sean el marco de protección.

Otra condición que asegura un interés legítimo del responsable es el descrito en el considerando (49), que establece al "responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a

> emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas".

De lo analizado, se concluye que la licitud es uno de los pilares fundamentales del andamiaje de la protección de datos personales, ya que el legislador prevé con anterioridad los casos o situaciones que justifican un régimen diferenciado ya sea maximizando las reglas de protección o permitiendo, por ejemplo, el tratamiento de datos sin necesidad de consentimiento del titular, por suplirlo el análisis previo del legislador que los determinó con criterio de ponderación, legitimidad y justicia.

6.5.4.9 Principio de tratamiento leal y transparente

Referencia de la noción actual del principio de tratamiento leal y transparente que ahora se localiza en el RGPD, consta, en la ya citada con anterioridad, sentencia del caso Google Spain y Google, emitida el 13 de mayo de 2014 y resuelta por el Tribunal de Justicia de la Unión Europea, en la cual este menciona que "incumbe al responsable del tratamiento garantizar que los datos personales sean tratados de manera leal y lícita"; respecto de la lealtad de manera puntual añade que "la exigencia de tratamiento leal de datos personales prevista en el artículo 6 de la Directiva 95/46 obliga a una administración pública a informar a los interesados de la transmisión de esos datos a otra administración pública para su tratamiento por ésta en su calidad de destinataria de dichos datos" lo que se presta para considerar que este principio, además de estar profundamente ligado al deber de información, tiene que ver con un marcado compromiso frente al titular de los datos.[732]

En ese contexto, el considerando (60) del RGPD establece los "principios de tratamiento leal y transparente por los cuales se exige que se informe al interesado de la existencia de la operación de tratamiento y sus fines"; de la "existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración" y si el titular está obligado a facilitar sus datos y las consecuencias en caso de que no lo hicieran.

Es decir, en concordancia con lo previamente mencionado, que estos principios se interrelacionan directamente con el deber de información, pues marcan las condiciones o características que la información debe cumplir, pues no basta la notificación desde el punto de vista formal, por la simple postura de asegurar que se cumplió con la comunicación, sino que es indispensable que la información esté dispuesta, entregada y contenga elementos que denoten el cumplimiento de la

[732] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-131/12, en el caso: Google Spain y Google], 2014, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES.

lealtad y transparencia en el actuar del responsable respecto de los datos y en su relación con el titular del dato.

Por eso, el mismo considerando (60) señala que "el responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente".

Cobra especial relevancia el considerando (61), que especifica como una manifestación evidente de la lealtad y de la transparencia, la relativa al momento en el que el responsable de tratamiento debe facilitar a los interesados la información sobre el procesamiento de sus datos personales, esto es en el mismo acto de recogida de los datos o, si se obtienen de otra fuente, "en un plazo razonable, dependiendo de las circunstancias del caso".

Este deber de lealtad y transparencia, conforme señala el mismo considerando (61), también se aplica a aquellos casos en los cuales "los datos personales pueden ser comunicados legítimamente a otro destinatario", el momento de informar al interesado es en el instante en el que se comunican al destinatario por primera vez.

En la doctrina se señala que "También hay que incluir la regla que impone la recogida leal de los datos. La lealtad en este terreno requiere el consentimiento informado del interesado o la cobertura de una autorización legal.[733]

En el mismo considerando se establece como criterio de lealtad y transparencia la obligación del "responsable del tratamiento que proyecte tratar los datos para un fin que no sea aquel para el que se recogieron debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y otra información necesaria".

Por lo analizado, se concluye con el artículo 5 del RGPD, que establece entre los principios relativos al tratamiento al de licitud, lealtad y transparencia, señalando expresamente que "1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado". Recoge en esta afirmación varios ámbitos y enfoques de aplicación que si bien son analizados y descritos en el considerando están abiertos a que sean un norte de actuación y no una limitación a casos específicos.

[733] P. L. MURILLO DE LA CUEVA, "La construcción del derecho a la autodeterminación informativa", *Revista de Estudios Políticos (Nueva Época)*, Núm. 104. Abril-Junio 1999, accedido el 11 de noviembre de 2019, 52

6.5.4.10 Principio de responsabilidad proactiva

Directamente asociado a las obligaciones del responsable de tratamiento se tiene al principio de responsabilidad proactiva por el cual, y conforme el considerando (74), debe constar en la normativa expresamente establecida cada uno de los deberes que deben cumplir respecto de cualquier tratamiento de datos personales realizado por él mismo o por su cuenta, es decir por otros o terceros en su nombre o por su orden o disposición. Por eso, el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en los apartados 1, 2 y 3 del artículo 4 del RGPD, y además deberá ser capaz de demostrarlo.

Dentro de las obligaciones que deben ser cumplidas por el responsable del tratamiento constan las siguientes:

a) Medidas oportunas y eficaces, que observen la naturaleza, ámbito, contexto y fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas, considerando (74)
b) Demostrable, esto es que pueda demostrar la conformidad de las actividades de tratamiento conforme la normativa, incluida la eficacia de las medidas (considerando [74]).
c) Medidas técnicas y organizativas apropiadas, como las de adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto (considerando [78]).
d) Reducir al máximo el tratamiento de datos personales (considerando [78]).
e) Seudonimizar lo antes posible los datos personales, (considerando [78]).
f) Transparentar las funciones y el tratamiento de datos personales (considerando [78]).
g) Facultar a los interesados supervisar el tratamiento de datos (considerando [78]).
h) Crear y mejorar elementos de seguridad (considerando [78]).
i) Privacidad por diseño y por defecto al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función (considerando [78]).
j) Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos (considerando [78]).
k) Mantener registros de las actividades de tratamiento bajo su responsabilidad (considerando [82]).
l) Cooperar con la autoridad de control y a poner a su disposición, previa solicitud, los citados registros, de modo que puedan servir para supervisar las operaciones de tratamiento (considerando [82]).

Conforme el considerando (75), se entiende por riesgos para los derechos y libertades de las personas físicas, aquellos tratamientos que pueden provocar daños y perjuicios físicos de gravedad y de probabilidad variables, materiales o inmateriales; en particular los casos que puedan dar lugar a discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo.

Las situaciones de vulnerabilidad que determinan mayores niveles de cuidado, y por tanto de responsabilidad, se encuentran determinadas en el mismo considerando 75 del RGPD, y se refieren a:

a) casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales;
b) datos sensibles: que revelan el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas;
c) crear o utilizar perfiles personales, para los cuales se evalúan aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos;
d) datos personales de personas vulnerables, en particular niños;
e) tratamiento de una gran cantidad de datos personales y afecte a un gran número de interesados.

Ahora bien, el considerando (76) del RGPD señala que además de estas condiciones de vulnerabilidad inherentes, es necesario analizar la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado desde la perspectiva del origen, la naturaleza, probabilidad, el alcance, la gravedad, el contexto y los fines del tratamiento de datos, y también ponderarse, sobre la base de una evaluación objetiva, si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

La normativa y las autoridades de protección pueden proporcionar directrices para la aplicación de medidas, con énfasis en la identificación del riesgo relacionado con el tratamiento, con las cuales el responsable o el encargado del tratamiento puede demostrar el cumplimiento o la identificación de buenas prácticas para mitigar el riesgo, que revistan ciertas circunstancias, en particular, conforme señala el considerando (77) del RGPD:

a) Códigos de conducta aprobados.
b) Certificaciones aprobadas.
c) Directrices dadas por el Comité Europeo de Protección de Datos (en adelante, el Comité) o indicaciones proporcionadas por un delegado de protección de datos.
d) El Comité también puede emitir directrices sobre operaciones de tratamiento que se considere improbable supongan un alto riesgo para los derechos y libertades de las personas físicas, e indicar qué medidas pueden ser suficientes en dichos casos para afrontar el riesgo en cuestión.

Reviste especial importancia lo señalado en el considerando (79) del RGPD por el cual, con la finalidad de que las autoridades de control puedan imputar niveles de responsabilidad, cumplan con

sus obligaciones de supervisión y dicten las medidas adecuadas, es necesario que los responsables y encargados del tratamiento realicen una atribución clara de las obligaciones, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable.

Finalmente, es indispensable acotar que la atribución de responsabilidad se realiza a sujetos pasivos, esto es a responsables de tratamiento, a encargados, al destinatario y al tercero, con las condiciones propias de cada caso. Anotándose que conforme señala el considerando (80) del RGPD, el representante es quien deberá asumir la responsabilidad dado que representa a la persona jurídica o mandante que ha realizado el tratamiento. Asimismo, lo hará el encargado siempre y cuando se cumpla con condiciones que califiquen la relación, como por ejemplo la existencia de un contrato, vínculo legal, mecanismo de adhesión o código de conducta que determine una relación debidamente especificada con la que pueda realizar un proceso de atribución específica de responsabilidades.

Como parte de este principio, la Guía del Reglamento General de Protección de Datos para responsables de tratamiento, expedida por la Agencia Española de Protección de Datos, Agencia Catalana de Protección de Datos, y Agencia Vasca de Protección de Datos, como mecanismo para orientar la actuación de los directamente afectados por el RGPD, reconoce un principio que denomina responsabilidad activa, por el cual es necesario que los responsables de tratamiento realicen actividades más allá de las que señala la normativa, pero que se deducen de ella, sobre todo desde la perspectiva de que son parte de su deber mínimo de cuidado, como por ejemplo las de documentar e identificar claramente la base legal sobre la que se desarrollan los tratamientos.

La citada Guía establece como ejemplos de esta responsabilidad las siguientes acciones:

> Hay que incluir la base legal sobre la que se desarrolla el tratamiento al proporcionar la información en el momento de recoger los datos de los interesados. Hay que especificar y documentar los intereses legítimos en que se fundamentan las operaciones de tratamiento en casos como las Evaluaciones de Impacto sobre la Protección de Datos o en determinadas transferencias internacionales. La identificación de la base legal es indispensable para estar en condiciones de demostrar que se cumple con las previsiones del RGPD. La identificación y documentación debe adaptarse al tipo de tratamiento y a las características de las organizaciones.[734]

[734] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, AGENCIA CATALANA DE PROTECCIÓN DE DATOS, Y AGENCIA VASCA DE PROTECCIÓN DE DATOS, «Guía del Reglamento General de Protección de Datos para responsables de tratamiento».

6.6 Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

6.6.1 Derecho de acceso

En el considerando (63) del RGPD consta uno de los derechos más importantes dentro del sistema integral de protección de los datos personales, el relativo al acceso. Por el cual, los interesados tienen "derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento".

Como antecedente, esta concepción del derecho al acceso recogida en el RGPD consta en la sentencia del caso Rijkeboer, emitida el 7 de mayo de 2009 y resuelta por el Tribunal de Justicia de la Unión Europea, acudiendo a los términos del Abogado General que señala que "los titulares de los datos tratados pueden velar por su buen uso, ejerciendo el llamado 'derecho de acceso' [...] pues el acceso representa la auténtica dimensión subjetiva de la Directiva, que, en suma, permite al individuo reaccionar en defensa de sus intereses".[735]

Este derecho se encuentra reconocido en el artículo 15 del RGPD, por el cual "el interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales". Ahora bien, el adelanto más importante en la concepción de este derecho es que no se limita al simple acceso a los datos personales, sino que en relación con el deber de información y el principio de finalidad, el titular también tiene derecho de acceso de la siguiente información:

a) los fines del tratamiento;
b) las categorías de datos personales de que se trate;
c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
f) el derecho a presentar una reclamación ante una autoridad de control;
g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información

[735] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-553/07., en el caso: Rijkeboer], 2009, accedido 13 de octubre de 2018, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62007CJ0553.

significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado;

i) cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia;
j) este derecho incluye el derecho de los interesados a acceder a "datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas" (considerando [63], RGPD).
k) facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales, siempre que el responsable esté facultado para ello (considerando [63], RGPD).
l) arbitrarse fórmulas para facilitar al interesado el ejercicio de los derechos de acceso, rectificación y supresión, así como el ejercicio del derecho de oposición de forma gratuita en el derecho como en el mecanismo. "El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas" (considerando [59], RGDP).

Otro de los avances en la definición del derecho de acceso consta en el número 3 del artículo 15 del RGPD, que determina los mecanismos prácticos mediante los cuales el responsable del tratamiento pondrá a disposición del titular una copia de los datos personales objeto de tratamiento a través de medios electrónicos o de otros medios físicos, "a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común".

Por su parte, el responsable tendrá derecho a solicitar ciertas condiciones mínimas que le permitan cumplir con el derecho del titular, las cuales son:

a) Percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos (art. 15, RGPD).
b) Solicitar que el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud, cuando se trata una gran cantidad de información relativa al interesado (considerando [63], GDPR).
c) Verificar la identidad de los interesados que soliciten acceso, en particular en el contexto de los servicios en línea y los identificadores en línea, utilizando todas las medidas razonables. "El responsable no debe conservar datos personales con el único propósito de poder responder a posibles solicitudes" (considerando [63], GDPR).

El derecho de acceso debe ponderarse con los derechos de terceros; es decir, "no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos. No obstante, estas consideraciones no deben tener como resultado la negativa a prestar toda la información al interesado" (considerando [63], RGPD).

6.6.2 Derecho de rectificación

La sección 3, denominada rectificación y supresión del RGPD, en el artículo 16 señala el derecho de rectificación, por el cual se otorga al interesado el derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan; además, a que se completen los datos personales, tomando en cuenta los fines del tratamiento, inclusive mediante una declaración adicional.

En el mismo sentido, el considerando (65) del RGPD señala que los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen.

Por su parte, el artículo 19 del RGPD señala que el responsable del tratamiento comunicará a cada uno de los destinatarios, cualquier rectificación o supresión de datos personales o limitación del tratamiento, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

La autoridad de control dispondrá de todos los poderes de investigación, entre ellos el relativo a ordenar la "rectificación o supresión de datos personales o la limitación de tratamiento y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales", al tenor del artículo 58, literal g) del RGPD.

Facilitar al interesado el ejercicio de los derechos de acceso, rectificación y supresión, así como el ejercicio del derecho de oposición de forma gratuita y por medios electrónicos especialmente cuando se traten por estos medios. Así como, "responder a las solicitudes del interesado a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas" (considerando [59], RGDP).

Sin embargo, es menester reconocer que este derecho ha presentado sus limitaciones, debido a situaciones que aunque parecen singulares, al Tribunal no le han sido ajenas; al respecto la sentencia del caso Nowak, emitida el 20 de noviembre de 2017 y resuelta por el Tribunal de Justicia de la Unión Europea respecto a la "rectificación" *a posteriori* de las respuestas de un examen menciona que "el carácter exacto y completo de los datos personales debe ser apreciado atendiendo a los fines para los cuales fueron recabados. En lo que se refiere a las respuestas de un aspirante en un examen, tales fines consisten en poder valorar la amplitud de sus conocimientos y competencias en la fecha del examen". Finalmente, cabe añadir que "tanto la Directiva 95/46 como el Reglamento

2016/679, que sustituyó a dicha Directiva, establecen determinadas limitaciones a estos derechos" cerrando con ello la posibilidad de que se cometan arbitrios dentro de su ejercicio.[736]

Además, al respecto de lo mencionado, la normativa interna de cada país, en concordancia con la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, puede imponer restricciones, establecer condiciones y garantías, procedimientos específicos, medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad, respecto de determinados principios y derechos; Por ejemplo, los de información, acceso, rectificación o supresión de datos personales, portabilidad de los datos, oposición, a las decisiones basadas en la elaboración de perfiles; así como a la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar:

a) la seguridad pública;
b) protección de la vida humana;
c) respuesta a catástrofes naturales o de origen humano;
d) la prevención, investigación y el enjuiciamiento de infracciones penales,
e) la ejecución de sanciones penales;
f) la protección frente a las amenazas contra la seguridad pública;
g) la protección frente a violaciones de normas deontológicas en las profesiones reguladas, y su prevención;
h) otros objetivos importantes de interés público, en particular un importante interés económico o financiero;
i) la llevanza de registros públicos por razones de interés público general;
j) el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios;
k) o la protección del interesado o de los derechos y libertades de otros;
l) la protección social, la salud pública y los fines humanitarios (considerando [73], RGPD);
m) con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos (considerando [156], RGPD). El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos.

Finalmente, el artículo 14 del RGPD, referido al derecho de información, determina que el responsable del tratamiento deberá facilitar al interesado, cuando los datos personales no se hayan obtenido directamente de él, información que permita garantizar un tratamiento de datos leal y transparente, esto es aquella relativa al derecho a solicitar del responsable el acceso a los datos personales, su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.

[736] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-434/16, en el caso: Nowak], 2017, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/document/document.jsf?docid=198059&doclang=ES&mode=req&occ=first.

6.6.3 Derecho de oposición

La sección 4, sobre el derecho de oposición y decisiones individuales automatizadas, consagra en el artículo 21 el derecho de oposición, mediante el cual, el interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento, incluida la elaboración de perfiles sobre la base de dichas disposiciones.

Como antecedente de esta concepción, marcada en el RGPD, consta en la sentencia ya citada del caso Google Spain y Google, emitida y resuelta por el Tribunal de Justicia de la Unión Europea, ya que al respecto señala que "los Estados miembros reconocerán al interesado el derecho a oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7 de la Directiva 95/46, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernen sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa". Además, menciona que "La ponderación que ha de efectuarse en el marco de dicho artículo 14, párrafo primero, letra a), permite así tener en cuenta de modo más específico todas las circunstancias que rodean a la situación concreta del interesado. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a estos datos."[737]

Continuando con el sentido del RGPD, el derecho de oposición del titular puede interponerse en cualquier momento cuando:

a) el tratamiento de datos personales tenga por objeto la mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines, a más tardar en el momento de la primera comunicación con el interesado;
b) se refiere a la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia;
c) en el contexto de la utilización de servicios de la sociedad de la información en el sector de las comunicaciones electrónicas, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas;
d) se traten con fines de investigación científica o histórica o fines estadísticos.

El interesado tendrá derecho a que se le informe explícitamente sobre los mecanismos para ejercitar el acceso, la rectificación, la supresión, así como el ejercicio del derecho de oposición al tratamiento, incluso la elaboración de perfiles en la medida que esté relacionado con mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y de forma gratuita y por medios electrónicos de ser el caso, al margen y de forma clara respecto de otra información, y cumplirse en el momento de la primera comunicación (considerandos (59) y (70), RGDP; art. 21, num. 3, RGPD).

[737] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-131/12, en el caso: Google Spain y Google], 2014, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES.

Conforme señala la citada normativa, el responsable del tratamiento podrá insistir con el tratamiento pese a la oposición del titular, y será él quien demostrará que sus intereses legítimos e imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado, lo que ocurre generalmente en los siguientes casos:

a) Acredite motivos legítimos imperiosos que prevalezcan sobre los intereses, los derechos y las libertades del interesado, asociados al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
b) Cuando los datos personales puedan ser tratados lícitamente y son necesarios para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero (considerando [69], RGPD).
c) Cuando el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (considerando [69], RGPD).
d) Para la formulación y el ejercicio o la defensa de reclamaciones.
e) Se traten con fines de investigación científica o histórica o fines estadísticos, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

6.6.4 Derecho de supresión y derecho al olvido digital

El artículo 17 del RGPD señala el derecho de supresión y a continuación coloca entre paréntesis otro nombre: derecho al olvido. Y esto se debe a que, tradicionalmente, el derecho de cancelación estaba exclusivamente dirigido a la supresión de información cuando se cumplían ciertas circunstancias relacionadas con la vigencia del tratamiento, el cumplimiento de la finalidad, la exactitud del dato y la autorización de la ley o el titular. Mientras que derecho al olvido se asociaba exclusivamente a la desindexación de información no relevante, sin repercusión en la memoria histórica ni afectación a la libertad de expresión que, sin embargo, causaba transgresiones a los derechos del titular. Asimismo, el derecho al olvido se refería exclusivamente a la desindexación de información personal que pudiera causar transgresiones. El motivo por el cual los dos se juntan en el mismo artículo radica en que las circunstancias que habilitan el derecho de cancelación son las mismas que permiten la desindexación. También las excepciones que permiten mantener la data y no eliminarla son las aplicables tanto al derecho de cancelación como al derecho al olvido. En consecuencia, se han unido dos derechos que si bien son diferentes comparten elementos en común: el derecho de cancelación consta desarrollado en el numeral 1 y el derecho al olvido, en el numeral 2 del citado artículo 17.

a) *Derecho de supresión:* Por el cual, el interesado tendrá derecho a que el responsable de tratamiento sin dilación indebida suprima los datos personales de su titularidad, cuando concurra alguna de las circunstancias siguientes:

    i. los datos personales ya no son necesarios para la finalidad para los que fueron recogidos o tratados de otro modo, es decir es necesario eliminar cuando se afecta a la finalidad o se ha incumplido el principio de lealtad y se ha tratado

datos de manera distinta a la que se solicitó su autorización inicial, artículo 17 RGPD;

ii. el interesado retire el consentimiento en que se basa el tratamiento el interesado para uno o varios fines específicos, artículo 6, numeral 1, literal a) del RGPD;

iii. el interesado se oponen al tratamiento de datos personales que les conciernen, considerando (65) RGPD;

iv. el interesado dio su consentimiento explícito para el tratamiento de datos sensibles con uno o más de los fines especificados, y este no se base en otro fundamento jurídico que permita retenerlos al responsable del tratamiento, artículo 9 numeral 2, literal a) del RGPD;

v. el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

vi. los datos personales hayan sido tratados ilícitamente, es decir se haya faltado al principio de legalidad y tratamiento legal y transparente;

vii. los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en la normativa y que se aplique al responsable del tratamiento;

viii. los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información de niños menores de 16, sin la autorización de quien ostenta la patria potestad o tutela, o de menos de 13 años, si en el país existe una norma que establezca esta edad como la mínima necesaria para la capacidad jurídica. Esta protección especial a los niños se debe a que ellos no están plenamente conscientes de los riesgos que implica el tratamiento. Además este derecho subsiste aun cuando el interesado ya no sea un niño, especialmente de datos que se alojan en internet (considerando [65], RGPD).

ix. si la retención de tales datos infringe el Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento (considerando [65], RGPD).

b) *Derecho al olvido:* El derecho al olvido "consiste en que las personas usuarias de Internet puedan obtener el borrado integral de sus datos personales y fotografías alojados en cualquier red social o manejados en internet por cualquier empresa. Este derecho puede entenderse incluido en la previsión constitucional referida al hábeas data, aunque su especificidad bien podría merecer un reconocimiento explícito, tal y como se ha planteado ya en el marco de la legislación de la Unión Europea".[738]

Es imperante añadir que este derecho tiene sus antecedentes en jurisprudencia emitida por el Tribunal de Justicia de la Unión Europea, específicamente en la sentencia del caso Google Spain y Google, emitida el 13 de mayo de 2014, en la que se exterioriza respecto de este derecho que "se tendrá que examinar, en particular, si el interesado tiene derecho a que la información relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre". A continuación añade: "estos derechos prevalecen, en principio, no sólo sobre el interés de dicho público en encontrar la mencionada información en una búsqueda que

[738] A. PÉREZ y B. i SERRAMALERA, *Curso de derecho constitucional*, 714.

verse sobre el interés de una persona" dándole con ello jerarquía ante el interés del responsable y del tercero que busca acceder a la información.[739]

Si el titular solicita la eliminación de los datos personales que un responsable haya hecho públicos, el responsable está obligado a eliminar los datos personales por cualquiera de las circunstancias antes descritas: por trasgresión a los principios de finalidad, licitud, lealtad, transparencia, consentimiento, entre otras. En este caso, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos los datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Para eso, el responsable del tratamiento deberá tomar en cuenta la tecnología disponible y el coste de su aplicación y adoptar medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos (considerando [66] y num. 2, art. 17, RGPD).

c) *Excepciones al derecho de cancelación y al derecho al olvido:* No se aplicará la cancelación o el derecho al olvido, lo cual posibilita la retención lícita de los datos personales por parte del responsable del tratamiento cuando es necesario para:

i. ejercer el derecho a la libertad de expresión e información;
ii. el cumplimiento de una obligación legal de un responsable del tratamiento que los requiera por imponerlo una normativa de la Unión Europea;
iii. el cumplimiento de una misión realizada en interés público;
iv. el ejercicio de poderes públicos conferidos al responsable;
v. el interés público en el ámbito de la salud pública; es decir, para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios; o cuando sea realizado por un profesional sujeto a la obligación de secreto profesional (art. 9, num. 2, lits. h) e i), y num. 3, RGPD);
iv. fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1 del RGPD, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento; o
v. para la formulación, el ejercicio o la defensa de reclamaciones.

Respecto de la normativa española, esto es la LOPDGDD y debido a que a través de esta se reconoce un catálogo de nuevos derechos digitales, el derecho al olvido aparece:

[739] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-131/12, en el caso: Google Spain y Google], 2014, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES.

> […] en dos preceptos de manera diferenciada lo que denomina el derecho al olvido en búsquedas de Internet y el derecho al olvido en servicios de redes sociales. Tradicionalmente el derecho al olvido se refería a aquellos supuestos en que los datos eran facilitados no por propio interesado sino por terceros (…) en este segundo supuesto estamos hablando tanto de datos personales que ha proporcionado el propio interesado para su publicación, como de datos facilitados por un tercero (…)[740]

En suma, la normativa española establece variantes del derecho al olvido, que amplían la protección del titular del dato no solo a buscadores sino a redes sociales y que a la larga se rigen por las mismas consideraciones y excepciones, pues debe garantizarse el respeto a la dignidad humana, pero también un adecuado interrelacionamiento con otros derechos como por ejemplo el acceso a información pública, la memoria histórica digital, el derecho de información, el derecho a la honra, entre otros.

6.6.5 Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

El artículo 22 del RGPD señala que **t**odo interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o le afecte significativamente de modo similar, como por ejemplo "la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna" (considerando [71], RGPD).

Conforme el citado artículo 22, numeral 2 del RGPD, es posible la decisión automatizada y, por ende, no procede este derecho cuando:

a) Es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; por ejemplo, para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento.
b) Está autorizada por el Derecho de la Unión o de los Estados miembros, siempre que se establezca medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; por ejemplo, para fines de control y prevención del fraude y la evasión fiscal.
c) Se basa en el consentimiento explícito del interesado.

En todo caso, el artículo 22 numeral 2 del RGPD y el considerando (71) del RGPD señalan que el tratamiento automatizado lícito siempre deberá cumplir con las garantías apropiadas, que incluyen:

[740] COMISIÓN JURÍDICA DEL CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA, *Op. Cit.*, 31-32

a) La adopción de medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.
b) Incluir la información específica al interesado.
c) Derecho a obtener intervención humana.
d) Derecho a expresar su punto de vista.
e) Derecho a recibir una explicación de la decisión tomada después de tal evaluación.
f) Derecho a impugnar la decisión.
g) Garantizar un tratamiento leal y transparente respecto del interesado.
h) Tener en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales.
i) Utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles.
j) Aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error.
k) Asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto.
l) Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares.

Respecto de datos sensibles, estos no podrán ser sometidos a tratamientos automatizados que generen decisiones que produzcan efectos jurídicos al titular, a menos que se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado y se cumplan una de las siguientes condiciones:

a) Se aplique consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando la normativa de la Unión o de sus Estados miembros lo prohíba, conforme el artículo 9, apartado 2, literal a) del RGPD.
b) El tratamiento es necesario por razones de un interés público esencial, conforme la normativa de la Unión o de sus Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado; conforme el artículo 9, apartado 2, literal g) del RGPD.

En todo caso no se admitirá tratamiento automatizados de menores de edad (considerando [71], RGPD).

Cabe destacar el alcance que manejaba la Directiva 95/46 en cuanto al tratamiento automatizado; al respecto consta la sentencia del caso Ryneŝ, emitida por el Tribunal de Justicia de la Unión Europea el 11 de diciembre de 2014, en la cual el Tribunal determina respecto de la grabación de imágenes

por parte de cámaras de vigilancia que "está comprendida, en principio, en el ámbito de aplicación de la Directiva 95/46/CE, en la medida en que constituye un tratamiento automatizado".[741]

Sin embargo, el almacenamiento de imágenes en video aun cuando fueran digitalizadas y automatizadas no producen por si solas valoraciones, a menos que se vinculan a datos biométricos del individuo. De tal manera que, para que este derecho opere no es suficiente que la información esté automatizada sino que producto de este proceso se realicen valoraciones que establezcan categorías que pudieran resultar perjudiciales para el titular.

6.6.*6* Derecho de consulta al registro general de protección de datos personales

En el Reglamento se concibe la obligación del responsable, del encargado o de sus representantes, de ser el caso, de realizar un registro de bases de datos efectuadas bajo su responsabilidad, para ponerlo a disposición de la autoridad de control que lo solicite (art. 30, num. 4, RGPD).

Téngase en cuenta que el citado reglamento no menciona el derecho de consulta por parte de un titular, derecho que si se reconoce en otras normativas latinoamericanas como la de Argentina, Colombia, Costa Rica, Guatemala, Perú, Nicaragua y Uruguay (véase 2.5.5.11, capítulo IV). Sin embargo, el numeral 5 del artículo 30 del RGPD señala que si la finalidad del registro es la consulta por parte de personas, solo podrán hacerlo los que tengan un interés legítimo.

El artículo 30 del RGPD señala que cada responsable y, en su caso, su representante llevarán un registro, por escrito, inclusive en formato electrónico, de las actividades de tratamiento efectuadas bajo su responsabilidad que no será notificada a la autoridad de control. Y que además, no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales sensibles, o datos personales relativos a condenas e infracciones penales.

a) *Registro realizado por el responsable:* El responsable de tratamiento o su representante legal deben registrar una base de datos que deberá contener toda la información que se indica a continuación:

   i. el nombre y los datos de contacto del responsable del corresponsable, del representante y del delegado de protección de datos;
   ii. los fines del tratamiento;
   iii. una descripción de las categorías de interesados;
   iv. una descripción de las categorías de datos personales;

[741] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [En el caso: Ryneŝ], 2017.

v. las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
vi. las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional, y en el caso de las transferencias internacionales basadas en una decisión de adecuación (art. 45, RGPD) o en medidas de garantías adecuadas (art. 46, RGPD), solo se podrá llevarse a cabo "si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales", al tenor de lo señalado en el artículo 49 del RGPD;
vii. cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
viii. cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad, apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, conforme el artículo 32 del RGPD.

b) *Registro realizado por el encargado:* Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

i. el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, del representante del responsable o del encargado, y del delegado de protección de datos;
ii. las categorías de tratamientos efectuados por cuenta de cada responsable;
iii. en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional; y en el caso de transferencias cuando no existe una decisión de adecuación, deberá constar la documentación de garantías adecuadas, la constancia de la transferencia y los intereses legítimos imperiosos perseguidos;
iv. cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

El artículo 49 del RGPD señala que una transferencia internacional es posible aun cuando no exista decisión de adecuación o medidas de garantías, de forma excepcional cuando desde un registro público que, conforme la ley, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero solo en la medida en que se cumplan, en cada caso particular, lo establecido en la normativa para la consulta. Pero no debe abarcar la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro, excepto si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo; en este caso la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

Ahora bien, el considerando (89) del RGPD recuerda que la Directiva 95/46/CE estableció la obligación general de notificar el tratamiento de datos personales a las autoridades de control, pero señala que esta medida implicó mucha carga administrativa y financiera, y en la práctica no contribuyó en todos los casos a mejorar la protección de los datos personales, sobre todo desde la perspectiva de seguridad.

Por lo tanto, el citado considerando (89) del RGPD propone que las obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren en:

i. los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas;
ii. las que implican el uso de nuevas tecnologías;
iii. son de una nueva clase de tecnologías y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativo a la protección de datos;
iv. si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial.

6.6.*7* Derecho a indemnización por daños causados

Desde la perspectiva del derecho a la indemnización por los daños y perjuicios causados en el tratamiento de los datos de carácter personal, el artículo 82 del RGPD y el considerando (146) establecen que "toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de un tratamiento en infracción del Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos".

Se aclara que además del titular del dato, puede presentar en su nombre una reclamación ante la autoridad de control, ejercer el derecho a la tutela judicial en nombre de los interesados, o ejercer el derecho a recibir una indemnización en nombre de estos, una entidad, organización o asociación sin ánimo de lucro constituida con arreglo al derecho de cada país que sea de interés público y actúe en el ámbito de la protección de los datos personales. Asimismo, un Estado miembro puede reconocer a una entidad, organización o asociación el derecho a presentar una reclamación con independencia del mandato de un interesado y del derecho a la tutela judicial efectiva, cuando existan motivos para creer que se han vulnerado los derechos de un interesado como consecuencia de un tratamiento de datos personales que sea contrario al Reglamento. Esa entidad, organización o asociación no puede estar autorizada a reclamar una indemnización en nombre de un interesado al margen del mandato de este último (considerando [142], RGPD).

Desde la perspectiva de la obligación de indemnizar, el artículo 82 y el considerando (146) del RGPD señalan que cualquier responsable o encargado del tratamiento, es decir quien participe en la

operación de tratamiento, deberá indemnizar daños y perjuicios que pueda sufrir una persona, por actos delegados y de ejecución, como consecuencia de un tratamiento que no cumpla o en infracción del Reglamento, o de otras normas de la Unión Europea, o de cada país miembro, o en el caso de los encargados haya actuado al margen o en contra de las instrucciones legales del responsable.

Cabe destacar que si los responsables o encargados participan en el mismo tratamiento, cada responsable o encargado debe ser considerado responsable de la totalidad de los daños y perjuicios. No obstante, si se acumulan en la misma causa, la indemnización puede prorratearse en función de la responsabilidad de cada responsable o encargado por los daños y perjuicios causados por el tratamiento, siempre que se garantice la indemnización total y efectiva del interesado que sufrió los daños y perjuicios. Todo responsable o encargado que haya abonado la totalidad de la indemnización puede interponer recurso posteriormente contra otros responsables o encargados que hayan participado en el mismo tratamiento, al tenor del artículo 82 y del considerando (146) del RGPD.

Lo importante es que los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos, independientemente que esta sea pagada por el responsable o el encargado, puesto que cada uno tendrá que asumir lo que le corresponda atendiendo su nivel de respectiva responsabilidad.

El responsable o el encargado deben quedar exentos de responsabilidad si se demuestra que no son responsables de modo alguno de los daños y perjuicios (art. 82, RGPD).

Respecto de la indemnización por violación de las normas corporativas vinculantes relativas al procesamiento de datos basados en un tratamiento automatizado, o en la elaboración de perfiles, los titulares tienen derecho a presentar una reclamación ante la autoridad de control y los tribunales competentes para obtener una reparación, y, cuando proceda, una indemnización, tal como consta en el artículo 47, numeral 2 e) del RGPD.

En el caso de inexistencia de una decisión de adecuación en trasferencia internacional de datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado, entre las cuales consta la de establecer derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país, de conformidad con lo señalado en el considerando (108) del RGPD.

Finalmente, respecto a las acciones judiciales, incluida la indemnización, contra un responsable o encargado del tratamiento serán aplicables tanto las normas establecidas en el Reglamento, como

las propias de competencia judicial establecidas en el Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo (considerando [147], RGPD). Para lo cual, el ejercicio del derecho a indemnización se presentará ante los tribunales competentes en el que el responsable o encargado tenga un establecimiento, o su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos (art. 79, apdo. 2, RGPD).

6.6.*8* Derecho a la confidencialidad

El derecho de confidencialidad aparece directamente relacionado con el derecho de seguridad, puesto que son complementarios, ya que los mecanismos adecuados —es decir medidas técnicas, administrativas, organizativas y jurídicas— que permiten la seguridad de la información tienen como consecuencia directa la confidencialidad de los datos personales. Inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento (considerando [39], RGPD).

El responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas que garanticen un nivel de seguridad adecuado, teniendo en cuenta la técnica y el coste con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse, para mitigarlos, garantizar la confidencialidad, la integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, de conformidad con lo señalado en el artículo 32 y considerando (83) del RGPD.

Dentro de los niveles de confidencialidad, la relativa al tratamiento de datos personales con fines estadísticos requiere que el control de accesos, las especificaciones y las medidas adecuadas para salvaguardar los derechos y las libertades de los interesados garanticen la confidencialidad estadística, al tenor de los señalado en el considerando (162) del RGPD.

El artículo 5, relativo a los principios relativos al tratamiento, determina que los datos personales serán: “f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)”. Es decir, se reconoce a la integridad y a la confidencialidad como principios propios del tratamiento de datos personales, anotándose que para el reglamento por confidencialidad se entiende a los mecanismos de seguridad adecuada que permita mantener la integridad del dato, pero sobre todo que no sea divulgada o puesta a disposición, sino únicamente de las personas que están autorizadas a su conocimiento y más aún tratamiento.

Por su parte, el artículo 28, numeral 3, señala que dentro de las obligaciones inherentes al encargado del tratamiento, que constarán en un contrato u otro acto jurídico, consta la de garantizar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

6.6.9 Spam

No existe en el RGPD mención alguna al *spam* o comunicaciones electrónicas no autorizadas.

6.6.10 Derecho a limitar el tratamiento

El derecho a limitar el tratamiento es una de las novedades de RGPD. Otras normativas tratan esta temática desde la perspectiva del bloqueo o de la suspensión asociada al principio de cancelación de datos. Este es el caso de países como Argentina, Colombia, Costa Rica, México, Nicaragua y Uruguay, en los cuales se establece que antes de tomar la decisión de eliminar un dato y durante el tiempo de deliberación, el dato personal debe bloquearse y dejar constancia de ello para informar sobre por qué no puede ser usado.

Antecedente de este título consta dentro de la sentencia del Tribunal de Justicia, de 22 de noviembre de 2012, correspondiente al caso Probst, la que menciona de manera explícita con respecto al tratamiento de los datos de tráfico que "sólo podrán encargarse [...] las personas que actúen bajo la autoridad del proveedor de [servicios] que se ocupen de la facturación [...], y dicho tratamiento deberá limitarse a lo necesario para realizar tal actividad".[742]

Ahora bien, en el caso del RGPD, según el artículo 18, el interesado tendrá derecho a obtener del responsable la limitación del tratamiento de los datos personales, no necesariamente cuando se va a solicitar su eliminación de un dato, sino que deberá producirse de cumplirse alguna de las condiciones siguientes:

a) *Impugnación sobre la exactitud:* Procederá a limitarse el tratamiento del dato personal y se verificará durante un plazo razonable, mientras se resuelve la impugnación sobre la exactitud de los datos personales.
b) *Impugnación sobre la ilicitud:* El tratamiento sea ilícito pero el interesado se opone a la supresión de los datos personales y en su lugar solicita la limitación de su uso.
c) *Necesidad de conservación:* En este caso, el responsable ya no necesita los datos personales para los fines del tratamiento; en cambio el interesado los necesita para formular acciones, o el ejercicio o la defensa de reclamaciones.
d) *Motivos legítimos:* El interesado que se opone al tratamiento solicita su eliminación, pero se pueden mantener los datos mientras se verifica si los motivos del responsable son legítimos y prevalecen sobre los del interesado.

El considerando (67) del RGPD aclara que entre los métodos para limitar el tratamiento de datos personales se pueden usar los siguientes:

[742] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-119/12, en el caso: Probst], 2012, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/document/document.jsf?docid=130242&doclang=ES

a) Trasladar temporalmente los datos seleccionados a otro sistema de tratamiento.
b) Impedir el acceso de usuarios a los datos personales seleccionados.
c) Retirar temporalmente los datos publicados de un sitio internet.
d) En ficheros automatizados, a través de medios técnicos de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse.

De otro lado, para que el responsable pueda superar la limitación impuesta por el interesado titular de los datos y pueda seguir tratando datos personales, es necesario el consentimiento del interesado, o que exista la necesidad de habilitar el tratamiento en razón del ejercicio o la defensa de los interesados, o con miras a la protección de los derechos de otra persona física o jurídica, o por razones de interés público.

Finalmente, existen varios deberes de información por parte del responsable, quien deberá:

a) informar al interesado que solicitó la limitación antes de que se produzca su levantamiento (art. 18, RGPD);
b) indicar, claramente, en el sistema sobre la limitación del tratamiento de los datos personales (considerando [67], RGPD).
c) comunicar a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado, la rectificación o supresión de datos personales, o en este caso la limitación del tratamiento (art. 19, RGPD);
d) informar, si es que el interesado lo solicita, acerca de los destinatarios a los que se hayan comunicado sobre una limitación en el tratamiento de datos personales o su levantamiento (art. 19, RGPD).

6.6.11 Derecho a la portabilidad

Respecto de la portabilidad, el artículo 20 del RGPD señala que el interesado tendrá derecho a recibir los datos personales que haya facilitado a un responsable del tratamiento y a transmitirlos a otro responsable del tratamiento directamente, sin que lo impida el responsable al que se los hubiera facilitado, cuando sea técnicamente posible.

Este derecho tiene la finalidad de "reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados" (considerando [68], RGPD).

Las características que deben cumplir los datos personales para que se considere efectivo el derecho a la portabilidad son las siguientes:

a) formato estructurado;
b) de uso común;
c) lectura mecánica;
d) con formatos interoperables que permitan la portabilidad de datos.

La portabilidad es posible cuando esté basada en el:

a) *Consentimiento:* Es decir, los datos personales pueden ser portables cuando exista consentimiento explícito para uno o varios fines específicos (art. 6, apdo. 1, lit. a), RGPD).
b) *Consentimiento de datos especiales:* Es decir, se admite el derecho a la portabilidad de categorías especiales de datos, como los relativos al origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física; siempre y cuando el Derecho de la Unión o de cada Estado miembro no prohíba el tratamiento de este tipo de datos, aun con anuencia de su titular (art. 9, apdo. 2, lit. a), RGPD).
c) *Relación y ejecución contractual:* La portabilidad de los datos es necesaria, tanto para la generación como para la ejecución de un contrato, si el interesado es parte de este o para la aplicación de medidas precontractuales(art. 6, apdo. 1, lit. b), RGPD).
a) *Medios automatizados:* Es posible la portabilidad cuando el tratamiento se efectúe por medios automatizados (art. 20, RGPD).

No será posible el cumplimiento del derecho de portabilidad cuando:

b) el tratamiento tiene una base jurídica distinta del consentimiento o el contrato (considerando [68], RGPD);
c) el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público (art. 20, RGPD);
d) el tratamiento sea necesario para el ejercicio de poderes públicos conferidos al responsable del tratamiento (art. 20, RGPD);
e) el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable (considerando [68], RGPD).

El derecho a la portabilidad de datos puede ser aplicado siempre que no se menoscabe el derecho de cancelación, el derecho al olvido y el de limitaciones al tratamiento. En particular no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato. Esta afirmación se debe a que el momento en el que se produce la portabilidad y un responsable traspasa a otro los datos, el primero debe borrarla de su

base de datos a menos que exista consentimiento del titular de que permanezca en esta o condición legal que impida el borrado o faculte la conservación.

El derecho a la portabilidad de datos no afectará negativamente a los derechos y libertades de otros ni aun cuando se refiera a un conjunto de datos personales determinado que concierna a más de un interesado.

Al tenor de los señalado en el considerando (68) del RGPD, el derecho del interesado a transmitir o recibir datos personales que le conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles, ya que la interoperabilidad debe estar en el formato mismo del dato cuya característica precisamente es la de ser interoperable.

Finalmente, la LOPDGDD española distingue entre el derecho a la portabilidad reconocido en el artículo 20 del RGPD de aquel derecho también denominado a la portabilidad pero que hace referencia a servicios de redes sociales y servicios de la sociedad de la información equivalente.

> […] Se trata de un nuevo derecho a la portabilidad que se reconoce más allá del derecho a la portabilidad de datos personales aportados por el interesado que está reconocido en el art. 20 del RGPD, si bien con ciertas limitaciones. Este derecho opera en relación con cualquier contenido que se hubiera facilitado por el interesado a los prestadores de los servicios de redes sociales y servicios de la sociedad de la información equivalentes, a los que se obliga a que los transmitan directamente a otro prestador que les haya sido indicado por el usuario pero solo si la transmisión es técnicamente posible. No obstante, no se facilitan criterios para determinar cuándo se considera que la transmisión es técnicamente posible y cuándo no, por lo que parece que en último término la garantía de este derecho queda en manos del proveedor, a diferencia de lo que ocurre con el derecho a la portabilidad de datos.[743]

De lo visto, el derecho a la portabilidad en servicios de redes sociales y servicios de la sociedad de la información equivalentes, reconocido en la normativa española, se considera un derecho diferente del derecho a la portabilidad de datos personales y por lo tanto, parte del catálogo de derechos digitales que establece la LOPDGDD.

6.6.12 Derecho de transparencia

El artículo 12 del RGPD, referido a la transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado, está estrechamente relacionado con el derecho de información de los titulares, y el deber de información de los responsables, pues en esta comunicación debe existir transparencia y lealtad.

[743] COMISIÓN JURÍDICA DEL CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA, *Op. Cit*., 29

En ese sentido, el derecho de transparencia presupone la prerrogativa que tiene toda persona de que el responsable del tratamiento tome medidas oportunas para facilitar al interesado toda información respecto de aquella información que debe ser puesta en conocimiento del titular en el momento de la recogida de datos y la obtención del consentimiento cuando se consigue del interesado (art. 13, RGPD), o de aquella que deberá facilitarse cuando no se hayan obtenido directamente del interesado (art. 14, RGPD).

La información que debe ser puesta en conocimiento del titular consta expresamente detallada en los citados artículos 13 y 14 del RGPD, principalmente corresponde a: la identidad y los datos de contacto del responsable y, en su caso, de su representante, los datos de contacto del delegado de protección de datos; los fines del tratamiento y la base jurídica del tratamiento; los nombres de los destinatarios o las categorías de destinatarios de los datos personales; la intención del responsable de transferir datos personales a un tercer país u organización internacional; el plazo durante el cual se conservarán los datos personales; si se ha obtenido consentimiento incluso en el caso de categorías especiales de datos; o cuando sea o no posible autorizar tratamiento de datos sensibles; se informará sobre el derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada, el derecho a presentar una reclamación ante una autoridad de control; si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos; la existencia de decisiones automatizadas, incluida la elaboración de perfiles, la importancia y las consecuencias previstas de dicho tratamiento; otras finalidades de tratamientos ulteriores, entre otras.

Además, la transparencia también gobierna las comunicaciones que se producen en el ejercicio de los derechos del titular reconocidos en los artículos 15 al 22 relativos al derecho de acceso, de rectificación, supresión, limitación al tratamiento, portabilidad de datos, oposición, decisiones individuales automatizadas, incluida la elaboración de perfiles y la violación de seguridad de los datos personales. De ese modo, la transparencia tiene varios ámbitos de aplicación propios del proceso de recogida y, por ende, tratamiento de la información como aquellos relativos a la presentación de reclamaciones del titular de los datos y el responsable del tratamiento.

Además, el considerando (58) del RGPD establece que el principio de transparencia también es aplicable a toda información dirigida al público en general, pues permite que la sociedad pueda acceder a información y comunicaciones que faciliten el ejercicio de sus derechos subjetivos de ser el caso. Dado que es "especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea", o en su defecto a solicitar cuentas y verificar las acciones diligentes, oportunas y probas tanto del Estado como de los particulares en su rol de responsables del tratamiento.

En consecuencia, la transparencia como derecho tiene varios enfoques característicos que deben ser observados para que su aplicación en los distintos ámbitos antes señalados permitan realmente cumplir con su finalidad: fortalecer al titular en el ejercicio de su autodeterminación informativa, incluido el control sobre sus datos; así como mejorar las relaciones de confianza y credibilidad entre titular y responsable, y en la generación de una sociedad que propugne una cultura de protección de los datos personales.

En ese sentido, el mismo considerando (58) del RGPD señala que la información que se dirija al público en general se requiere que cumpla con las siguientes características:

a) Concisa.
b) Fácilmente accesible.
c) Fácil de entender.
d) Utilice un lenguaje claro y sencillo.
e) Se visualice, de ser el caso.
f) Facilitarse en forma electrónica, si es el caso, por ejemplo, cuando esté dirigida al público, mediante un sitio web.
g) Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

Ahora bien, el artículo 12 del RGPD señala las características y condiciones que debe tener la información sobre el tratamiento de datos personales, así como en las comunicaciones propias del ejercicio de los derechos del titular y de la interrelación entre el responsable de tratamiento y los titulares, para que se consideren transparentes, las cuales son:

a) Concisa.
b) Transparente.
c) Inteligible.
d) De fácil acceso.
e) *Gratuita:* Siempre y cuando las solicitudes no sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo; en estos casos el responsable podrá cobrar un canon razonable en función de los costes administrativos o negarse a actuar respecto de la solicitud. Pero será el responsable quien deberá probar lo infundado o excesivo de la solicitud.
f) *Lenguaje claro y sencillo:* En particular aquella información dirigida específicamente a un niño.
g) *Facilidad en la entrega de información:* Tanto si es por escrito como por otros medios, inclusive si procede por medios electrónicos. Incluso verbal, siempre que se demuestre la identidad del interesado por otros medios.
h) *Información adicional:* Cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa solicitud de las reconocidos en los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

i) *Iconos normalizados*: Podrá transmitirse información en "combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible en una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente" (art. 12, RGPD.

Como todas las actuaciones que se asocian al responsable del tratamiento deben respetar la debida diligencia, resulta obvio pensar que aquellas características propias de la información dirigida al público en general también son aplicables a la información propia de la relación entre el responsable y el titular en la recogida de datos como en las comunicaciones para el ejercicio del derecho y viceversa.

6.6.13 Restricciones a las obligaciones, los derechos y los principios

El RGPD establece un artículo específico que señala limitaciones aplicables a las obligaciones, los principios y derechos que son parte del derecho a la protección de datos personales. Las limitaciones establecidas en la ley resultan ser un mecanismo muy útil para determinar cuál es el contenido mínimo del derecho, en este caso del derecho a la protección de datos personales.

Una las finalidades de determinar el contenido esencial es la de identificar los casos de excepción que ameritan una versión acotada del derecho sin que sea posible eliminar elementos considerados esenciales pero sí otros que si bien ayudan a su desarrollo su omisión no significa un irrespeto al derecho en sí mismo.

Este es el caso de lo dispuesto en el artículo 23 del RGPD, denominado "Limitaciones", por el cual el Derecho de la Unión o de los Estados miembros -incluida la Carta y el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales-, aplicable a los responsables o al encargado del tratamiento, podrá limitar mediante medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 (acceso, rectificación, supresión, derecho al olvido, oposición, portabilidad, limitación al tratamiento, no soportar decisiones individuales automatizadas, incluida la elaboración de perfiles), así como las contenidas en el artículo 34 relativas a las notificaciones de las violaciones de seguridad y las del artículo 5, respecto a los principios en su relación con los citados derechos y obligaciones, incluso en aquellas conexas.

Esas limitaciones son posibles únicamente si se respetan en lo esencial los derechos y libertades fundamentales y se constituyan en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar: la seguridad del Estado, la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano; la defensa, la prevención, investigación, detección o enjuiciamiento o ejecución de infracciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención; otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular

un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; la llevanza de registros públicos por razones de interés público general; el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios, o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios; la protección de la independencia judicial y de los procedimientos judiciales; la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública; la protección del interesado o de los derechos y libertades de otros; la ejecución de demandas civiles, conforme consta en el artículo 23 y en el considerando (73) del RGPD.

Es decir, constan expresamente y de forma taxativa aquellas excepciones que justifican un régimen acotado al contenido esencial del derecho, todas ellas ponderadas previamente por el legislador, desde la perspectiva de que prima el bien común y el interés general en cuanto al derecho a la protección de datos personales individual.

Al respecto, consta como antecedente la sentencia del caso *Volker und Markus Schecke y Eifert*, emitida el 9 de noviembre de 2010, en la cual se menciona que las limitaciones o restricciones "deben establecerse sin sobrepasar los límites estrictamente necesarios" en función de que "cabe concebir medidas que entrañen lesiones de menos gravedad a este derecho fundamental de las personas físicas, sin dejar por ello de contribuir eficazmente al logro de los objetivos de la normativa de la Unión".[744]

La referida medida legislativa contendrá como mínimo —y en este caso el RGPD establece— el contenido esencial del derecho a la protección de datos personales en las siguientes disposiciones específicas:

a) la finalidad del tratamiento o de las categorías de tratamiento;
b) las categorías de datos personales de que se trate;
c) el alcance de las limitaciones establecidas;
d) las garantías para evitar accesos o transferencias ilícitas o abusivas;
e) la determinación del responsable o de categorías de responsables;
f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento;
g) los riesgos para los derechos y libertades de los interesados, y
h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

[744] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-283/11, en el caso: Volker und Markus Schecke y Eifert], 2010, accedido 13 de octubre de 2018, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62011CC0283

De lo transcrito, se concluye que es parte del contenido esencial mínimo aquellos elementos relacionados con la naturaleza del dato, el objeto o bien jurídico en el que consta el derecho de información, la autodeterminación informativa y la necesidad de mandato legal, así como los principios de finalidad, de licitud, de conservación, determinación de los sujetos activos y pasivos, y los derechos.

6.7 Obligaciones generales

El RGPD establece en el capítulo IV, denominado Responsable del tratamiento y encargado del tratamiento, cinco secciones que desarrollan las obligaciones que estos sujetos pasivos deben. Estas secciones marcan una innovación en la forma de concebir la responsabilidad y los mecanismos reales que se proponen para verificar el compromiso y nivel de cumplimiento de quienes tratan datos personales.

La sección 1, relacionada con las obligaciones generales, contiene sobre lo referente a la responsabilidad del responsable del tratamiento (art. 24); la protección de datos desde el diseño y por defecto (art. 25); sobre los corresponsables del tratamiento (art. 26); los representantes de responsables o encargados del tratamiento no establecidos en la Unión (art. 27); sobre el encargado del tratamiento (art. 28); el tratamiento bajo la autoridad del responsable o del encargado del tratamiento (art. 29); registro de las actividades de tratamiento (art. 30), y sobre la cooperación con la autoridad de control (art. 31). En suma, esta sección recoge desde el enfoque de criterios generales, principios y derechos las obligaciones propias específicas que asumen los responsables del tratamiento y los encargados.

La sección 2 de este capítulo hace referencia a la seguridad de los datos personales y la seguridad del tratamiento (art. 32); la notificación de una violación de la seguridad de los datos personales a la autoridad de control (art. 33); la comunicación de una violación de la seguridad de los datos personales al interesado (art. 34). Es decir, se aborda la seguridad desde una obligación del responsable y del encargado del tratamiento, aunque consta de forma expresa en el artículo 5, literal f), del RGPD el principio de seguridad adecuada por el cual los datos deben ser tratados de tal manera que se garantice la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas que precautelen su integridad y confidencialidad. Sobre este tema, se analizó en el numeral 6.5.4.3 del presente capítulo.

Acerca de la sección 3, sobre la evaluación de impacto de la protección de datos y consulta previa, esta debida diligencia que consta en el artículo 35 sobre evaluación de impacto de la protección de datos, y en el artículo 36 relativo a la consulta previa, propone una nueva forma de asumir la carga de tratar los datos respetando los derechos humanos, denominada responsabilidad demostrada.

La sección 4, sobre el delegado de protección de datos, establece como obligación de los responsables el establecimiento y designación de este representante de los intereses del titular del dato y garante de los derechos de los titulares, así como un mecanismo de preparación y evaluación para los organismos públicos o privados del complimiento de la normativa. Los artículos 36, 37, 38 y 39 sobre las funciones y designación y posición del delegado de protección de datos.

La sección 5, por su parte, establece los códigos de conducta y certificación mediante los cuales se propone mejorar las relaciones entre titular y sujeto pasivo, de tal manera que el artículo 40 desarrolló la temática de los códigos de conducta; en el artículo 41 está lo relativo a la supervisión de los citados códigos de conducta; el artículo 42 sobre la certificación, y el artículo 43 respecto del organismo de certificación.

De la estructura de este capítulo, se colige que el gran cambio de paradigma que propone el RGPD deviene del estado actual de la técnica y su vertiginoso desarrollo que acrecienta los riesgos y la gravedad de los posibles daños que pueden causarse a los derechos y libertades de las personas físicas y del papel fundamental que los sujetos pasivos tienen en la naturaleza, ámbito, contexto y fines del tratamiento. Por lo que los responsables y encargados deben asumir, acoger y cumplir medidas técnicas, organizativas apropiadas e incluir, de ser el caso, políticas de protección de datos, a fin de garantizar y demostrar que el tratamiento es realizado conforme con el Reglamento, y evidencia de que se pueden desarrollar innovaciones, emprendimientos al mismo tiempo que el respeto y la garantía de derechos de las personas, lo que se denomina responsabilidad demostrada. Dichas medidas se revisarán y actualizarán cuando sea necesario (art. 24, RGPD).

La adhesión a códigos de conducta o la implementación de mecanismos de certificación podrán ser utilizadas como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Es necesario, entonces, analizar las obligaciones y compromisos que los responsables de tratamiento y encargados, en razón de los fenómenos sociales asociados a la revolución tecnológica, deben asumir como manifestación pragmática de su parte para el cumplimiento del objeto o bien jurídico, de los principios y de los derechos desarrollados en el citado RGPD.

6.7.1 Corresponsables del tratamiento

Cuando dos o más responsables determinen los objetivos y los medios del tratamiento, serán considerados corresponsables del tratamiento, a menos que de modo transparente y de mutuo acuerdo consten sus respectivas responsabilidades, funciones y relaciones en el cumplimiento de las obligaciones impuestas por el Reglamento, el derecho de la Unión y de los Estados miembros, en particular en cuanto al ejercicio de los derechos del interesado y del deber de información, la designación un punto de contacto para los interesados y la puesta en conocimiento de los interesados de los aspectos esenciales del acuerdo. Los responsables aun cuando exista un acuerdo

podrán ejercer sus derechos frente a, y en contra de, cada uno de los responsables (art. 26, RGPD). El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite (art. 31).

Ya sea encargado del tratamiento o cualquier persona que actúe bajo la autoridad del responsable o del encargado, solo podrá tratar datos personales bajo las instrucciones del responsable, a no ser que estén obligados a ello en virtud de una normativa expresa (art. 29). Cabe anotar que su nivel de responsabilidad aumenta si un encargado del tratamiento infringe el Reglamento al determinar los fines y medios del tratamiento, ya que se aplica una presunción, y es la de ser considerado responsable del tratamiento con respecto a dicho tratamiento (art. 28, RGPD).

6.7.2 Cláusulas contractuales tipo

Para definir que se entienden por cláusulas contractuales se ha dicho que son aquellas que:

> […] se hallan configuradas por el derecho comunitario como una prueba de que concurren garantías adecuadas con respecto las transferencias internacionales de datos. Existen dos tipos de cláusulas aquellas en las que el importador es el responsable y aquellas en las que el importador es el encargado. En ambos casos el exportador siempre es un responsable, aunque el GT29 ha adoptado en 2014 un proyecto de cláusulas que deben insertarse en el que tanto el exportador como el importador sean los encargados de tratamiento. Las cláusulas contractuales tipo contienen una declaración jurídicamente exigible en virtud de la cual tanto el "exportador de datos" como el "importador de datos" se comprometen a tratar los datos de conformidad con las normas básicas de protección de datos (es decir, el respeto a la privacidad y a los derechos y libertades fundamentales de los individuos) y están de acuerdo que puedan ejercitar sus derechos en virtud de contrato. Pueden verse incluidas en un contrato mucho más amplio. - No impiden que sus responsables adopten cláusulas contractuales *ad hoc* adaptadas a su situación concreta. Sus características más importantes son: - Una cláusula de terceros beneficiarios que permita a los usuarios ejercer derechos contractuales aunque no sean parte del contrato. - El destinatario o importador de datos acuerda someterse al procedimiento de la Autoridad Nacional de Control del Estado del responsable de la exportación de datos y/o de los tribunales en caso de conflicto. Las cláusulas presentan cierta rigidez, lo que les convertían en menos interesantes que el antiguo sistema del Puerto Seguro y pueden ser difícil de aplicación por los Tribunales no comunitarios dado que pueden no estar familiarizados con la compleja normativa de protección de datos de la UE.[745]

Estas cláusulas suelen ser usadas en transferencias internacionales de datos. El artículo 46 y el considerando (108) del RGPD establecen que el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país. Estas medidas pueden ser normas corporativas vinculantes o a cláusulas tipo de

[745] F. GUDÍN RODRÍGUEZ-MAGARIÑO, *Nuevo Reglamento Europeo de Protección de Datos vs Big Data*, (Valencia: Tirant lo Blanch on line, 2018)

protección de datos adoptados por la Comisión o por una autoridad de control, o a las cláusulas contractuales autorizadas por una autoridad de control.

Cualquiera de los citados mecanismos tiene como finalidad asegurar que los derechos y principios de la protección de datos se respeten en el tratamiento de datos personales. Para lo cual, deberán mostrarse al titular de los datos, los derechos exigibles, las posibles acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización.

La autoridad de control podrá adoptar cláusulas contractuales tipo para regular todos los contenidos mínimos que debe tener la relación jurídica entre encargado y responsable; las que deberán constar por escrito, inclusive en formato electrónico.

6.7.3 Protección de datos desde el diseño y por defecto

El considerando (78) del RGPD señala que la obligación del responsable del tratamiento de es adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. En este sentido, el artículo 25 del RGPD establece que, tomando en cuenta "el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas", el responsable del tratamiento o el encargado deberán cumplir con lo siguiente:

1. *Medidas desde el diseño:* A fin de cumplir con los requisitos contemplados en el considerando (78), como en el artículo 25 del RGPD, debe proteger los derechos de los interesados, integrar las garantías necesarias en el tratamiento y aplicar de forma efectiva los principios de protección de datos; deberán aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas como:

    a) *Seudonimización*, tomando en cuenta que debe implementarse lo antes posible.
    b) Reducir al máximo el tratamiento de datos personales, minimización de datos.
    c) Dar transparencia a las funciones y el tratamiento de datos personales.
    d) Permitir a los interesados supervisar el tratamiento de datos.
    e) Permitir al responsable del tratamiento crear y mejorar elementos de seguridad.
    f) Los principios de la protección de datos desde el diseño, y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

2. *Medidas por defecto:* Deberán aplicarse medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento:

    a) Los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.
    b) Que no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
    c) Se aplique a la cantidad de datos personales recogidos.
    d) Se aplique a la extensión de su tratamiento.
    e) Se aplique a su plazo de conservación.
    f) Se aplique a su accesibilidad.

3. *Promover la protección de datos desde el diseño y por defecto:* El considerando (78) del RGPD establece la obligación de alentar a los productores a tomar en cuenta el derecho a la protección de datos cuando desarrollan y diseñen sus productos, servicios y aplicaciones. Pero, además, que se aseguren que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos, sobre todo en atención del estado de la técnica, de los costos, de la naturaleza, ámbitos, fines y de los posibles riesgos a los derechos de los titulares de estos tratamientos. En el mismo sentido, se deberá motivar a los consumidores organizaciones y/o personas naturales a seleccionar y usar productos, servicios y aplicaciones que estén basados en el tratamiento de datos personales por diseño y por defecto.

4. *Mecanismo de certificación:* Como establece el artículo 42 del RGPD, podrá utilizarse un mecanismo de certificación aprobado que acredite el cumplimiento en las operaciones de tratamiento de los responsables y los encargados de la privacidad por diseño y por defecto.

6.7.4 Códigos de conducta

Se entienden por código de conducta aquellas normas que regulan la actuación de responsables y encargados del tratamiento para el cumplimiento de los deberes, derechos y principios de la protección de datos personales, atendiendo las cuestiones particulares de cada sector especializado y sus características propias y específicas respecto del tratamiento y de las necesidades específicas de las microempresas y las pequeñas y medianas empresas, al tenor del considerando (98) y del artículo 40 del RGPD.

Dichos códigos de conducta establecerán obligaciones de los responsables y encargados, teniendo en cuenta, el riesgo probable que se derive del tratamiento para los derechos y libertades de las personas físicas (considerando [98], RGPD).

La adhesión del encargado del tratamiento a un código de conducta aprobado o a un mecanismo de certificación podrá utilizarse como elemento para demostrar que se ha elegido a un encargado o este

ha recurrido a otro encargado que se ha tomado en cuenta que ofrecen garantías suficientes para aplicar medidas técnicas y organizativas apropiadas para del tratamiento, conforme el RGPD, el Derecho de la Unión y de los Estados miembros (considerando [81]).

A continuación se desarrollará los elementos mínimos para la puesta en funcionamiento de los códigos de conducta:

1. *Actores que deben promover la elaboración de códigos de conducta*

El artículo 40 del RGPD establece la obligación de promover la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del Reglamento a los siguientes actores:

a) Estados miembros de la Unión Europea.
b) Las autoridades de control.
c) El Comité.
d) La Comisión.

2. *De la elaboración, la modificación o ampliación de código de conductas*

Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos.

Las asociaciones y otros organismos que representan a categorías de responsables o encargados del tratamiento deberán consultar a las partes interesadas, incluidos los interesados cuando sea posible, y tener en cuenta las consideraciones transmitidas y las opiniones manifestadas en respuesta a dichas consultas (considerando [99], RGPD).

Los elementos que deberán ser especificados en los códigos de conducta son:

a) el tratamiento leal y transparente;
b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;
c) la recogida de datos personales;
d) la seudonimización de datos personales;
e) la información proporcionada al público y a los interesados;
f) el ejercicio de los derechos de los interesados;

g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;
h) las medidas y procedimientos del responsable del tratamiento;
i) las medidas y procedimientos para aplicar la privacidad por diseño y por defecto;
j) las medidas y procedimientos para garantizar la seguridad del tratamiento;
k) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;
l) la transferencia de datos personales a terceros países u organizaciones internacionales;
m) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos;
n) los procedimientos para presentar una reclamación ante una autoridad de control, conforme el artículo 77 del RGPD;
o) los procedimientos para presentar acciones judiciales ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento, tutela judicial efectiva (art. 79, RGPD);
p) mecanismos que permitan a un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente (art. 41, num. 1, RGPD) a efectuar el control obligatorio del cumplimiento de las disposiciones del citado código de conducta, sin perjuicio de las funciones y los poderes de las autoridades de control competente.

3. *Procedimiento de aprobación de elaboración, modificación o ampliación de códigos de conducta:*

Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento presentarán el proyecto de código o la modificación o ampliación ante la autoridad de control competente (art. 55, RGPD), quien dictaminará si el proyecto está conforme con el reglamento; de tal manera que lo aprobará, lo registrará y publicará si considera suficientes las garantías adecuadas ofrecidas (art. 40, RGPD). Si un proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros, lo presentará por el procedimiento denominado mecanismo de coherencia que consta en el artículo 63, por el cual un Comité emitirá un dictamen aprobatorio ante la Comisión, si dicho proyecto, modificación o ampliación se encuentra conforme con el Reglamento u ofrece garantías adecuadas en el caso trasferencias internacionales. Por su parte, la Comisión podrá, mediante actos de ejecución, decidir que el código de conducta o la modificación o ampliación aprobados y presentados tienen validez general dentro de la Unión, de tal manera que lo publicitará y archivará en un registro para ponerlos a disposición pública por cualquier medio apropiado (art, 40, nums. 9, 10 y 11, RGDP).

4. *De la adhesión a los códigos de conducta:*

Podrán adherirse a un código de conducta aprobado previamente:

a) Los responsables o encargados del tratamiento a los que se aplica el reglamento.
b) Los responsables o encargados a los que no se aplica el Reglamento, por no estar incursos en lo dispuesto en el artículo 3, relativo al ámbito de aplicación territorial de este reglamento.

5. *Requisitos para la adhesión a códigos de conducta de responsables o encargados a los que no se aplica el Reglamento*

Los responsables o encargados a los que no se aplica el Reglamento, por no serles aplicable el ámbito de aplicación territorial del mismo, podrán adherirse a códigos de conducta aprobados siempre y cuando:

a) Se asuman en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales.
b) Asuman compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, al responsable o encargados del tratamiento en el tercer país, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.
c) El código de conducta se encuentre aprobado por la autoridad de control competente si considera suficientes las garantías adecuadas ofrecidas, al tenor de lo dispuesto en el artículo 40 del RGPD.
d) Que el código de conducta tenga validez general, mediante actos de ejecución por parte de la Comisión, que establezcan que tienen validez general dentro de la Unión, si considera las garantías como adecuadas (art. 40, nums. 8 y 9, RGPD).

6. Supervisión de códigos de conducta aprobados

El artículo 41 del RGPD establece que los códigos de conducta aprobados podrán ser supervisados por:

a) La autoridad de control competente; sobre la composición, competencia, funciones, procedimientos se verá en el acápite correspondiente.
b) Los organismos que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.

7. Organismo acreditado con pericia en el objeto del código

El artículo 41 del RGPD señala que sin perjuicio de las funciones y los poderes de la autoridad de control competente, podrán supervisar el cumplimiento de un código de conducta un organismo acreditado con pericia en el contenido del código. De modo que, sin perjuicio de las funciones y los poderes de la autoridad de control competente, deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente.

a) *Acreditación:*

Para su acreditación por parte de una autoridad competente, el organismo deberá:

i. Demostrar a satisfacción, su independencia y pericia en relación con la protección de datos personales en el respectivo código.
ii. Haber establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código.
iii. Haber establecido procedimientos que le permitan supervisar el cumplimiento de las disposiciones del código.
iv. Haber establecido procedimientos que le permitan examinar periódicamente la aplicación del código.
v. Haber establecido procedimientos y estructuras transparentes para tratar las reclamaciones relativas a infracciones del código.
vi. Haber establecido procedimientos y estructuras transparentes para evidenciar la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento.
vii. Haber establecido procedimientos y estructuras transparentes para los interesados y el público.
viii. Haber demostrado, a satisfacción, que sus funciones y cometidos no dan lugar a conflicto de intereses con la autoridad de control.

b) Procedimiento para aprobación y revocatoria de un organismo acreditado con pericia en el objeto del código

i. La autoridad de control competente presentará al Comité, mediante el mecanismo de coherencia del artículo 63 del RGPD, el proyecto que fija los criterios de acreditación de un organismo.
ii. La autoridad de control competente revocará la acreditación de un organismo si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el Reglamento.
iii. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos.

6.7.5 Certificación en materia de protección de datos y de sellos y marcas de protección de datos

Se entiende por mecanismos de certificación y de sellos y marcas de protección de datos en las operaciones de tratamiento, aquellos que permiten aumentar la transparencia y el cumplimiento del Reglamento; que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes (considerando [100], RGPD) y demostrar el cumplimiento de lo dispuesto en el RGPD por parte de responsables y encargados, tomando en cuenta las necesidades específicas de las microempresas, las pequeñas y medianas empresas, al tenor de lo dispuesto en el artículo 42 del RGPD:

1. *Actores que deben promover la elaboración de certificados, sellos y marcas de protección de datos*

El artículo 42 del RGPD establece la obligación de promover la elaboración de mecanismos de certificación en materia de protección de datos, sellos y marcas de protección de datos destinados a contribuir a la correcta aplicación del Reglamento a los siguientes actores:

a) Estados miembros de la Unión Europea.
b) Las autoridades de control.
c) El Comité.
d) La Comisión.

2. *Del sometimiento a certificados, sellos y marcas de protección de datos*

a) Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento a los que se aplica el RGPD podrán someterse a certificados, sellos y marcas de protección de datos para demostrar la existencia de garantías adecuadas.
b) Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento a los que no rige el presente RGPD, por no serles aplicable el ámbito de aplicación territorial de este reglamento contemplado en el artículo 3, podrán someterse a certificados, sellos y marcas de protección de datos para demostrar la existencia de garantías adecuadas cuando:

a. Sean aplicables para el marco de transferencias de datos personales a terceros países u organizaciones internacionales.
b. Se asuman compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

3. *Requisitos para someterse a certificaciones, sellos o marcas de protección de datos*

Conforme señala el artículo 42 de RGPD, los responsables y encargados deberán cumplir con los siguientes requisitos para someterse a certificaciones, sellos o marcas de protección de datos:

a) El sometimiento a la certificación, sellos o marcas sea voluntaria.
b) El sometimiento a la certificación, sellos o marcas esté disponibles a través de un proceso transparente.

4. *Responsabilidades del responsable y del encargado cuando ostente una certificación, sellos o marcas de protección de datos*

a) La certificación no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del RGPD.
b) La certificación no limitará las funciones y los poderes de las autoridades de control.
c) Los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos serán responsables de la correcta evaluación a efectos de certificación o retirada de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento del Reglamento.

5. *Autoridades u organismos competentes que expidan o revoquen certificaciones, sellos o marcas de protección de datos:* El artículo 43 señala las autoridades u organismos que expidan o revoquen certificaciones, sellos o marcas de protección de datos:

a) Los órganos de control competente: Sobre estos se tratará en el acápite correspondiente.
b) El Comité: Cuando se trate de mecanismos de coherencia dará lugar a una certificación común: el Sello Europeo de Protección de Datos. El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado (art. 42, RGPD).
c) Los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos Sobre estos se realizará un análisis pormenorizado a continuación (art. 43, RGPD).

6. *De los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos:* Los Estados miembros garantizarán que los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos cumplan con lo siguiente:

a) Serán acreditados por uno o por ambos de los siguientes entes:

a. Autoridad de control que sea competente.
b. Organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, 9 de julio de 2008, por el cual se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008)[746] con arreglo a la norma en ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control.
c. La Comisión estará facultada para adoptar actos delegados, para especificar las condiciones que deberán tenerse en cuenta en los mecanismos de certificación en materia de protección de datos, conforme el artículo 43 numeral 8. La Comisión podrá adoptar actos de ejecución que establezcan normas técnicas para promover y reconocer mecanismos de certificación y los sellos y marcas de protección de datos. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

b) Los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos, al tenor de lo dispuesto en el artículo 43 del RGPD, serán acreditados si:

a. Han demostrado, a satisfacción de la autoridad de control competente, su independencia y su pericia en relación con el objeto de la certificación, al tenor del Reglamento (CE) 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008.[747]
b. Se han comprometido a respetar los criterios que han habilitado certificaciones emitidas por otros organismos de certificación, o por autoridades de control competentes o por el Comité.
c. Han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificaciones, sellos y marcas de protección de datos.
d. Han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación.
e. Han establecido procedimientos y estructuras para verificar la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento.
f. Han establecido procedimientos y estructuras transparentes para los interesados y el público.
g. Han demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.
h. La acreditación de los organismos de certificación se realizará sobre la base de los criterios aprobados por la autoridad de control competente, o por el Comité de conformidad con el artículo 63. Los mismos que complementarán con lo dispuesto en el Reglamento (CE) 765/2008 y las

[746] PARLAMENTO EUROPEO Y DEL CONSEJO DE EUROPA, *Reglamento (CE) 765/2008, 9 de julio de 2008 por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) 339/93*, 9 de julio de 2008, 20, https://www.boe.es/doue/2008/218/L00030-00047.pdf., 30.
[747] PARLAMENTO EUROPEO Y DEL CONSEJO DE EUROPA, 20, 30.

normas técnicas que describen los métodos y procedimientos de los organismos de certificación.

c) La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada.
d) La autoridad de control hará públicos los requisitos para la acreditación de organismos de certificación y los criterios de acreditación previstos por las autoridades de control o por el Comité en una forma fácilmente accesible.
e) Las autoridades de control comunicarán los requisitos y criterios al Comité.
f) La autoridad de control competente o el organismo nacional de acreditación revocará la acreditación a un organismo de certificación si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo de certificación infringe el Reglamento.
g) Los organismos de certificación comunicarán a las autoridades de control competentes las razones de la expedición de la acreditación como organismos o de su retirada.

7. *Procedimiento para establecer o revocar certificaciones, sellos o marcas de protección de datos*

El artículo 42 del RGPD instaura el procedimiento para que se establezca o se revoquen certificaciones, sellos o marcas de protección de datos a favor de responsables o encargados de tratamiento de conformidad con lo siguiente:

a) La autoridad de control o los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones, una vez informada la autoridad de control, a fin de que esta pueda ejercer, retirar una certificación u ordenar al organismo de certificación que retire una certificación que no cumpla con lo dispuesto en los artículos 42 y 43 del RGPD, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación.
b) Los responsables o encargados que sometan su tratamiento al mecanismo de certificación entregarán al organismo de certificación toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.
c) La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años.
d) La certificación podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes.
e) La certificación será retirada, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación.

6.7.6 Evaluación de impacto relativa a la protección de datos

Las evaluaciones de impacto sobre la protección de datos personales son una de innovaciones del Reglamento europeo, porque van de la mano de la responsabilidad demostrada, ya que establecen

un mecanismo previo y proactivo tanto para el responsable, como para el encargado y para las autoridades de control de verificar los tratamientos que pudieran causar perjuicio a sus titulares antes de que se produzcan. El considerando (84) señala que se establece este mecanismo con la finalidad de mejorar el cumplimiento del Reglamento.

A continuación se revisará la forma en la que se deberá llevar a cabo la evaluación en el citado reglamento.

1. *Circunstancias que obligan a realizar evaluaciones de impacto*

Acorde a lo dispuesto en el considerando (90) y del artículo 35 del RGPD, el responsable de tratamiento deberá realizar, antes del tratamiento, una evaluación de las operaciones y de impacto del tratamiento en la protección de datos, con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta si:

a) Se van a utilizar nuevas tecnologías.
b) La naturaleza, alcance, contexto o fines, entrañen un alto riesgo para los derechos y libertades de las personas físicas.
c) Se va a realizar una evaluación sistemática y exhaustiva de aspectos personales de personas físicas, que se realizan mediante un tratamiento automatizado, a través de la elaboración de perfiles, o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas, cuyas decisiones pueden tener efectos jurídicos o afecten significativamente respecto de personas físicas concretas (considerando [91], RGPD).
d) Se va a realizar un tratamiento a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales.
e) Se van a realizar operaciones de tratamiento a gran escala que persiguen una cantidad considerable de datos personales a escalas regional, nacional o supranacional y que podrían afectar a un gran número de interesados, porque, por ejemplo, hacen más difícil para los interesados el ejercicio de sus derechos (considerando [91], RGPD).
f) Se va a realizar una observación sistemática a gran escala para el control de una zona de acceso público, en particular cuando se utilicen dispositivos optoelectrónicos.
g) Para cualquier otro tipo de operación cuando la autoridad de control competente considere que el tratamiento entrañe probablemente un alto riesgo para los derechos y libertades de los interesados; en particular porque:

    a. impida a los interesados ejercer un derecho;
    b. utilizar un servicio;
    c. ejecutar un contrato;
    d. porque se efectúe sistemáticamente a gran escala. No debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o

clientes, un solo médico, otro profesional de la salud o abogado (considerando [91], RGPD).

2. *Procedimiento para realizar evaluación de impacto*

El procedimiento que debe seguirse para realizar una evaluación de impacto relativa a la protección de datos, según el artículo 35 del RGPD es el siguiente:

a) Se podrá realizar una única evaluación que podrá abordar una serie de operaciones de tratamiento que entrañen altos riesgos similares. Esto por cuanto el considerando (92) señala que hay circunstancias en las cuales puede ser razonable y económico que una evaluación de impacto "abarque más de un único proyecto, por ejemplo, en el caso de que las autoridades u organismos públicos prevean crear una aplicación o plataforma común de tratamiento, o si varios responsables proyecten introducir una aplicación o un entorno de tratamiento común en un sector o segmento empresarial o para una actividad horizontal de uso generalizado".
b) El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos.
c) El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados.
d) La autoridad de control establecerá, publicará y comunicará al Comité Europeo de Protección de Datos (creado en el artículo 68 del RGPD) las listas sobre:

    a. Los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos.
    b. Los tipos de operaciones de tratamiento que por cumplir los criterios previamente analizados, obligatoriamente requieran una evaluación de impacto relativa a la protección de datos.
    c. Antes de adoptar las citadas listas, la autoridad de control deberá aplicar el mecanismo de coherencia previsto en el artículo 63 del RGPD, cuando en estas se incluyen actividades de tratamiento que guarden relación con:

        i. la oferta de bienes o servicios a interesados;
        ii. la observación del comportamiento de estos en varios Estados miembros;
        iii. actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

e) Recabar la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento, cuando proceda.

3. *Contenido del informe de evaluación de impacto*

El informe de evaluación de impacto relativo a la protección de datos personales deberá incluir como mínimo:

a) Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento.
b) El interés legítimo perseguido por el responsable del tratamiento, de ser el caso.
c) Una evaluación de la necesidad de las operaciones de tratamiento con respecto a su finalidad.
d) Una evaluación de la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.
e) Una evaluación de los riesgos para los derechos y libertades de los interesados.
f) Las medidas previstas para afrontar los riesgos.
g) Las garantías, medidas de seguridad y mecanismos para mitigar riesgos y que garanticen la protección de datos personales, con miras a demostrar el cumplimiento del Reglamento.
h) En el análisis tomar en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.
i) Se deberá tomar en cuenta, al evaluar las repercusiones de las operaciones de tratamiento realizadas por responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos el cumplimiento de los códigos de conducta aprobados, referidos en el artículo 40.
j) El responsable de considerarlo necesario examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, cuando exista un cambio del riesgo que representen las operaciones de tratamiento (art. 35).

4. *Evaluación de impacto de tratamiento previsto para cumplir con obligaciones legales, o realizadas por interés público o ejercicio de poderes públicos*

Cuando el tratamiento se realice en virtud de una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, y tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, no será necesario cumplir con lo señalado previamente excepto si la normativa de cada Estado miembro considera necesario proceder a dicha evaluación previa a las actividades de tratamiento. Según el considerando (93), los Estados miembros creen necesario llevar a cabo dicha evaluación con carácter previo a las actividades de tratamiento debido.

5. *Obligaciones del encargado de tratamiento respecto de evaluaciones de impacto*

El encargado del tratamiento a petición del responsable debe asistirle cuando sea necesario, a fin de asegurar que se cumplen las obligaciones que se derivan de la realización de las evaluaciones de impacto relativas a la protección de datos y de la consulta previa a la autoridad de control, conforme el considerando (95).

6. *Obligación de consulta previa ante informes negativos de evaluación de impacto*

Los considerandos (84) y (94) y el artículo 36 del RGPD estipulan la obligatoriedad de consultar a la autoridad de control antes de iniciar las actividades de tratamiento si existe una evaluación negativa de impacto relativa a la protección de datos, en especial cuando entrañen un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debiéndose consultar a la autoridad de control antes del tratamiento.

Además, esta evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el Reglamento.

Sobre los requisitos, condiciones, procedimientos y características propias de la consulta previa, se tratarán en el siguiente acápite.

6.7.7 Consulta previa

Como se señaló en líneas precedentes, la consulta previa es un mecanismo que obliga al responsable de tratamiento a consultar a la autoridad de control cuando un informe de evaluación de impacto de protección de datos tuvo resultados negativos y existen indicios que, de realizarse el tratamiento, este podría causar perjuicios a los titulares de los datos. En este sentido, a continuación se desarrolla los contenidos propios que permiten el desarrollo de esta nueva figura jurídica establecida en el RGPD.

1. *Circunstancias que obligan a realizar una consulta previa a la autoridad de control*

Conforme el artículo 36 del RGPD, el responsable consultará obligatoriamente a la autoridad de control, antes de proceder al tratamiento, cuando:

a) Una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo.

b) En ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas.
c) El responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación.
d) Existe la probabilidad de que ese alto riesgo se deba a determinados tipos de tratamiento y al alcance y frecuencia de este, lo que también puede ocasionar daños y perjuicios o una injerencia en los derechos y libertades de la persona física.

2. *Procedimiento de la consulta previa*

El procedimiento constará desarrollado en la normativa de cada Estado miembro; sin embargo, sus criterios generales constan en el considerando (94) y en el artículo 36 del RGPD al tenor de lo siguiente:

a) La autoridad de control debe responder a la solicitud de consulta dentro de un plazo determinado en las normativas internas de cada Estado miembro.
b) La ausencia de respuesta de la autoridad de control dentro de dicho plazo no impide que dicha autoridad pueda intervenir basada en sus funciones y poderes, incluido el poder de prohibir operaciones de tratamiento.
c) Como parte del proceso de consulta, se puede presentar a la autoridad de control el resultado de una evaluación de impacto relativa a la protección de datos efectuada en relación con el tratamiento en cuestión, en particular las medidas previstas para mitigar los riesgos para los derechos y libertades de las personas físicas. Esto con la finalidad de verificar si la autoridad con esta información adicional autoriza o no el tratamiento.
d) Cuando la autoridad de control considere que el tratamiento previsto podría infringir el Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá:

    a. En un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de los poderes de investigación previstos en el artículo 58 del RGPD.
    b. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto.
    c. La autoridad de control informará al responsable o al encargado de los motivos que facultan la prórroga, en el plazo de un mes a partir de la recepción de la solicitud de consulta.
    d. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

3. *Información que puede requerirse del responsable para emitir la resolución de consulta previa*

Para emitir el informe que corresponda, la autoridad de control podrá solicitar al responsable del tratamiento la siguiente información, quien la facilitará de forma obligatoria:

a) Las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial, de ser el caso.
b) Los fines y medios del tratamiento previsto.
c) Las medidas y garantías establecidas para proteger los derechos y libertades de los interesados.
d) Los datos de contacto del delegado de protección de datos.
e) La evaluación de impacto relativa a la protección de datos.
f) Cualquier otra información que solicite la autoridad de control.

4. *Consulta previa para medidas legislativas*

Durante la elaboración de toda propuesta de medida legislativa o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento, los Estados miembros garantizarán que se consulte a la autoridad de control. En este sentido, el considerando (96) señala que deben llevarse también a cabo consultas con la autoridad de control, a fin de garantizar la conformidad entre la norma de cada país y lo dispuesto en el RGPD y mitigar el riesgo que implique el tratamiento para el interesado.

5. *Consulta previa sobre tratamientos previstos para cumplir con obligaciones legales, o realizadas por interés público o ejercicio de poderes públicos*

Será facultativo de cada Estado miembro establecer en su derecho una obligación a los responsables relativa a consultar a la autoridad de control y recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público; en particular el tratamiento en relación con la protección social y la salud pública (art. 36, RGPD).

6.7.8 Registro de las actividades de tratamiento

De conformidad con el artículo 30 del RGPD para facilitar el trabajo de control de la autoridad es necesario realizar el registro de las actividades de tratamiento.

Si bien, en la derogada normativa española, Ley 4633/1999 LOPD se señalaba que se debía registrar ficheros de datos protegidos, la nueva normativa, en su artículo 31 LOPDGDD, en cumplimiento de lo dispuesto en el artículo 30 del RGPD, determina que:

> […] cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad (…) Del mismo modo, cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable (…)[748]

El registrar tratamientos es una evidente evolución en el sistema de protección, ya que no son solo ficheros con sus finalidades específicas los que marcan la intervención de un órgano de control sino la integralidad de los datos de una entidad que pueden ser tratados de diversas maneras, con finalidades, tecnologías y niveles de seguridad diferentes.

6.8 Encargado del tratamiento que ofrezca garantías suficientes

Como se analizó en el numeral relativo a sujetos pasivos del derecho a la protección de datos personales. El encargado del tratamiento es quien trata datos personales por cuenta del responsable del tratamiento, artículo 4, numeral 8) del RGPD.

> Por tanto la figura del encargado de tratamiento es muy amplia, incluyendo, entre otros, a empresas de marketing, gestorías contables, empresas de hosting, empresas de servicios informáticos, delegado de protección de datos externo y, de manera general, a cualquier persona física o jurídica que preste algún tipo de servicio que conlleve el tratamiento de datos de carácter personal por cuenta del responsable del fichero.[749]

Esta figura tiene antecedentes de mención en la jurisprudencia del Tribunal de Justicia de la Unión Europea, específicamente en la sentencia emitida correspondiente al caso Digital Rights Ireland y Seitlinger y otros. En ella, respecto a las reglas relativas a la seguridad y a la protección de los datos conservados, se exterioriza que "la Directiva 2006/24 no contiene garantías suficientes, como las que exige el artículo 8 de la Carta, que permitan asegurar una protección eficaz de los datos conservados contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos respeto de

[748] C. CAMPOS ACUÑA, "Los 10 «imprescindibles» en protección de datos para las administraciones públicas (RGPD Y LOPDGDD)", *La Ley*, volumen 828, (2018), accedido el 16 de noviembre de 2019, http://elconsultor.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAiMzYxMzA7Wy1KLizPw8WyMDQwsDQyNTkEBmWqVLfnJIZUGqbVpiTnEqAIJrf9M1AAAAWKE

[749] F. GUDÍN RODRÍGUEZ-MAGARIÑO, *Nuevo Reglamento Europeo de Protección de Datos vs Big Data*, (Valencia: Tirant lo Blanch on line, 2018)

tales datos". Esto lleva a entender de manera más específica la necesidad que impulsó la exigencia de esta categoría.[750]

El artículo 28, numeral 3, señala que el tratamiento por parte del encargado se regirá por un contrato u otro acto jurídico que cumpla con la normativa de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, las obligaciones y derechos del responsable incluida la confidencialidad.

Es obligación del responsable elegir para el tratamiento de datos personales únicamente, al encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, todo ello para garantizar tanto el cumplimiento del RGPD y la protección de los derechos del interesado (art. 27, RGPD).

6.8.1 Formalidades en la elección de otros encargados

El encargado del tratamiento no podrá recurrir a otro encargado sin que medie autorización previa por escrito, específica o general, por parte del responsable que le ha designado. De producirse algún cambio en la incorporación o sustitución de otros encargados, se informará al responsable, dando así al responsable la oportunidad de oponerse. Si el encargado recurre a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico válido, las mismas condiciones previstas entre el encargado original y el responsable, en particular aquellas relativas a la prestación de garantías suficientes de medidas técnicas y organizativas. Si ese otro encargado incumple sus obligaciones, el encargado inicial seguirá siendo plenamente responsable (art. 27, RGPD).

Dentro de las responsabilidades proactivas del responsable de tratamiento y en cuanto a su obligación de nombrar a un encargado de tratamiento se ha dicho que:

> Según el RGPD, el responsable, de conformidad con el principio de responsabilidad activa, deberá adoptar medidas apropiadas, incluida la elección de encargados, de forma que garantice y esté en condiciones de demostrar que el tratamiento se realiza conforme a la normativa de protección de datos. Los responsables habrán de elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento. Esta

[750] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C283/11, en el caso: Digital Rights Ireland y Seitlinger y otros], 2014, accedido 13 de octubre de 2018, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CJ0293

previsión se extiende también a los encargados cuando subcontraten operaciones de tratamiento con otros subencargados. [751]

6.8.2 Contenido mínimo del contrato del encargado

El contrato u otro acto jurídico entre responsable y encargado se regirá conforme la normativa de la Unión o de cada Estado miembro y del presente artículo 27 del RGPD. Entre su contenido mínimo tendrá lo relativo al objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Además, dicho contrato o acto jurídico estipulará de forma expresa que el encargado debe:

1. Tratar datos personales siguiendo exclusivamente las instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo obligación legal que se aplique al encargado, quien informará al responsable, previo al tratamiento, de esa exigencia legal, salvo la normativa lo prohíba por razones importantes de interés público.
2. Garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.
3. Tomar todas las medidas de seguridad necesarias.
4. Respetar las formalidades para elección de otros encargados que ofrezcan garantías suficientes.
5. Asistir al responsable, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para responder a las solicitudes de ejercicio de los derechos de los interesados.
6. Ayudar al responsable a garantizar el cumplimiento de las obligaciones de seguridad, de notificación de una violación de la seguridad a la autoridad de control y al interesado; realizar, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento que, de resultar pertinente, habilitará a realizar una consulta previa ante el organismo de control y vigilancia.
7. Suprimir o devolver todos los datos personales, a petición del responsable, una vez finalizada la prestación de los servicios de tratamiento, y suprimir las copias existentes a menos que se requiera la conservación de los datos personales de conformidad con la ley.
8. Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, y para permitir la realización de auditorías, inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable. El encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el RGPD.
9. Sin perjuicio de que entre responsable y encargado se celebre un contrato individual, podrá basarse, total o parcialmente, en las cláusulas contractuales tipo inclusive de aquellas dispuestas en la ley.

[751] F. GUDÍN RODRÍGUEZ-MAGARIÑO, *Nuevo Reglamento Europeo de Protección de Datos vs Big Data*, (Valencia: Tirant lo Blanch on line, 2018)

De otro lado, desde la perspectiva de responsabilidad proactiva se señala que:

> Así el Considerando 81 del RGPD establece que la adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos. Los encargados pueden adherirse a códigos de conducta o certificarse en el marco de los esquemas de certificación previstos por el RGPD. [752]

De lo transcrito, se concluye que los contratos entre responsable y encargado, los códigos de conducta o las certificaciones permiten determinar de manera precisa las obligaciones de responsable, las del encargado y en suma las interrelaciones entre ellos, las cuales atienden a evitar problemas y en el caso de que estos se susciten facilitar el establecimiento de responsabilidades.

6.8.3 Representantes de responsables o encargados del tratamiento no establecidos en la Unión

Cuando se realice el tratamiento de datos personales por parte de un responsable o encargado no establecido en la Unión, y siempre que dicho procesamiento esté relacionado con la oferta de bienes o servicios a dichos interesados, independientemente de si a estos se les requiere su pago, o se refiera al control del comportamiento, en la medida en que este tenga lugar en Europa, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión, en uno de los Estados miembros en que estén los interesados cuyos datos personales se tratan, para que atienda las consultas. No será necesario nombrar este representante si se realiza por parte de autoridades u organismos públicos o se refiere a un tratamiento ocasional, siempre y cuando no incluya una gran escala de categorías especiales de datos, no sean de datos personales relativos a condenas e infracciones penales, sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas. Los interesados podrán ejercer acciones ante el representante sin perjuicio de las que pudieran emprenderse contra el propio responsable o encargado (art. 27, RGPD).

[752] F. GUDÍN RODRÍGUEZ-MAGARIÑO, *Nuevo Reglamento Europeo de Protección de Datos vs Big Data*, (Valencia: Tirant lo Blanch on line, 2018)

De otro lado, tanto si se trata de encargados ubicados dentro o fuera de la Unión Europea, las responsabilidades que deben cumplir podrán estar recogidas en contratos entre responsables y encargados, así como también en la normativa constante en el RGPD, tal como se señala en el siguiente texto:

> En determinadas materias los encargados tienen obligaciones propias que establece el RGPD, que no se circunscriben al ámbito del contrato que los une al responsable, y que pueden ser supervisadas separadamente por las autoridades de protección de datos. Por ejemplo: - Deben mantener un registro de actividades de tratamiento. - Deben determinar las medidas de seguridad aplicables a los tratamientos que realizan. - Deben designar a un DPO en los casos previstos por el RGPD. [753]

6.9 Procedimientos

El RGPD establece en el capítulo VIII, los recursos, responsabilidad y sanciones que permiten la exigibilidad de este instrumento normativo. Al respecto, el citado Reglamento determina varios mecanismos de solicitud o de reclamación atendiendo a la autoridad, la persona a la que se dirigirá o el tipo de decisión de la que se interpone una acción, los cuales son:

6.9.1 Mecanismos para solicitar acceso, rectificación, supresión u oposición directamente al responsable o encargado del tratamiento

De conformidad con el considerando (59) del RGPD y el artículo 12, numeral 3, se debe facilitar al interesado el ejercicio de sus derechos, entre ellos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. A continuación, los elementos necesarios para el análisis de este tipo de mecanismos:

1. *Sujeto activo:*

Se entenderá como sujeto activo de estos derechos al interesado.

[753] F. GUDÍN RODRÍGUEZ-MAGARIÑO, *Nuevo Reglamento Europeo de Protección de Datos vs Big Data*, (Valencia: Tirant lo Blanch on line, 2018)

2. *Sujeto pasivo:*

Se entenderá como sujeto pasivo al responsable del tratamiento o su encargado.

3. *Derechos tutelados:*

Se consideran tutelados los derechos acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición, reconocidos desde el artículo 15 al 22 del RGPD.

4. *Procedencia:*

Esta solicitud procede en aplicación del artículo 12 relativa al derecho de transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado. Ya que el responsable del tratamiento deberá tomar medidas oportunas para facilitar al interesado información prescrita en los artículos 13 y 14 relativos a la información que debe facilitarse cuando los datos se obtienen o no directamente del interesado, así como cualquier comunicación para facilitar que el interesado pueda ejercitar los derechos reconocidos en los artículos del 15 al 22 del RGPD.

5. *Procedimiento:*

En el caso de los derechos del titular, reconocidos en los artículos del 15 al 22, el responsable facilitará al interesado información relativa a sus actuaciones en el plazo de un mes a partir de la recepción de la solicitud, que podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes; indicará los motivos de la dilación, por medios electrónicos cuando sea posible, a menos que solicite de otro modo.

Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

El responsable del tratamiento deberá proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos (art. 12, num. 1, RGPD).

6.9.2 Derecho a presentar una reclamación ante una autoridad de control única

El artículo 77 del RGPD establece el derecho a presentar una reclamación ante una autoridad de control con la finalidad de que sea esta la que, investida de sus poderes de investigación, pueda impedir que se siga produciendo la violación a la normativa sobre el tratamiento de datos y el responsable rectifique su actuación.

1. *Sujeto activo:*

   Se considera sujeto activo a todo interesado que tenga derecho a presentar una reclamación. Se entiende por interesado a la persona física identificada e identificable, excluyéndose de esta manera de forma expresa a las personas jurídicas (art. 4, num. 1).

   De conformidad con el artículo 80 y el considerando (142) del RGPD, el interesado podrá actuar en un procedimiento por intermedio de un representante que el designe a su arbitrio mediante mandato, quien presentará en su nombre la citada reclamación. Pero de conformidad con el RGPD, este representante deberá ser una entidad, organización o asociación sin ánimo de lucro, correctamente constituida, cuyos objetivos estatutarios sean de interés público, actúe en el ámbito de la protección de los derechos y libertades en especial de la protección de sus datos personales.

   Asimismo, cualquier Estado miembro, si considera que los derechos del interesado han sido vulnerados por parte de un tratamiento, podrá disponer que la entidad, organización o asociación a la que se hace referencia en el párrafo anterior, tenga con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control (art. 80 y considerando [142], RGPD).

2. *Sujetos pasivos u obligados*

   Se entienden como sujetos pasivos u obligados aquellos que deberán responsabilizarse por las violaciones o transgresiones reclamadas; estos son los siguientes:

3. *Los responsables del tratamiento o su representante:*

   Es la persona física o jurídica, pública o privada, servicio u otro organismo nacional o internacional que, solo o en conjunto, determine los fines y medios del tratamiento, ya sea que cuente o no con un representante designado por escrito que lo represente respecto a las obligaciones señaladas en el RGPD. Cabe anotar que, de conformidad con el artículo 27, la designación de un representante por parte del responsable se

entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable.

4. *Los encargados del tratamiento o su representante:*

Es la persona física o jurídica, pública o privada, servicio u otro organismo nacional o internacional que trate datos personales por cuenta y bajo autoridad directa del responsable del tratamiento. En el caso de que el encargado tenga representante, se le aplica todo lo señalado en el acápite anterior.

5. Derechos tutelados

El citado artículo 77 señala que el interesado podrá interponer reclamación si considera que el tratamiento de sus datos personales ha infringido el RGPD. De manera general, se consideran afectados los derechos de acceso, rectificación, supresión, derecho al olvido, limitación al tratamiento, portabilidad de datos, notificación de violación de seguridad, derecho de oposición y sobre decisiones individuales automatizadas, incluida la elaboración de perfiles reconocidos en los artículos 15 al 22 y el 34 del RGPD, así como a los principios reconocidos en el artículo 5 del RGPD, en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22.

6. Procedencia

Esta reclamación procede sin perjuicio de cualquier otro recurso administrativo o acción judicial que se haya presentado.

7. Procedimiento

La reclamación será presentada ante la autoridad de control, en particular la del Estado miembro en el que el interesado tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción.

La autoridad de control, ante la que se haya presentado la reclamación, informará al reclamante sobre el avance y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial, conforme el artículo 78.

Respecto de los casos de *litisdependencia*, se establece que si un tribunal competente de un Estado miembro tiene información sobre "acciones vinculadas entre sí por una relación tan estrecha que procede tramitarlas y resolverlas conjuntamente a fin de evitar resoluciones que podrían ser incompatibles si se sustanciaran como causas separadas" (considerando [144], RGPD).

Es decir, si existe un procedimiento que por tener el mismo asunto en relación con el tratamiento y el mismo responsable o encargado en razón de las partes intervinientes podrán unirse los procedimientos. Para tal efecto, dicho tribunal se pondrán en contacto con el otro del Estado miembro para confirmar la existencia de dicho procedimiento. De ser verdadera la información, cualquier tribunal competente distinto de aquel ante el que se ejercitó la acción en primer lugar podrá suspender su procedimiento. Si dicho procedimiento está pendiente en primera instancia, cualquier tribunal distinto de aquel ante el que se ejercitó la acción en primer lugar podrá también, a instancia de una de las partes, inhibirse en caso de que el primer tribunal sea competente para su conocimiento y su acumulación sea conforme a Derecho (art. 81).

6.9.3 Derecho a la tutela judicial efectiva contra una autoridad de control

Antecedente de este derecho se encuentra determinado en la sentencia de 29 de enero de 2008, resuelta y emitida por el Tribunal de Justicia de la Unión Europea, correspondiente al caso *Promusicae*, cuyo pronunciamiento respecto a la tutela judicial efectiva menciona que "el derecho fundamental de propiedad, del que forman parte los derechos de propiedad intelectual, como los derechos de autor [...] y el derecho fundamental a una tutela judicial efectiva constituyen principios generales del Derecho comunitario".[754]

El artículo 78 reconoce el derecho a la tutela judicial efectiva contra una autoridad de control. De modo que un interesado puede accionar esta tutela una vez que no haya sido contestada o se haya dictado una decisión jurídicamente vinculante que haya negado o desestimado total o parcialmente una reclamación previa, presentada ante una autoridad de control de conformidad con lo previsto en el artículo 77, previamente analizado, o no actúe cuando sea necesario para proteger los derechos del interesado:

1. *Sujeto activo*

Se considera sujeto activo a toda persona física o jurídica que tiene derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control.

[754] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C275/06, en el caso: Promusicae], 2008, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/liste.jsf?language=es&num=C-275/06

El interesado mediante mandato podrá designar a una entidad, organización o asociación sin ánimo de lucro, cuyos estatutos tengan por objetivo el ámbito de la protección de los derechos y libertades en especial de la protección de sus datos personales, o para que cualquier Estado miembro disponga directamente a cualquiera de estos órganos se presente tutela judicial efectiva contra la autoridad de control, de considerarse existe algún tipo de vulneración a los datos personales (art. 80, RGPD, y considerando [142], RGPD).

2. Sujetos pasivos u obligados

Serán sujetos pasivos u obligados los mismos que fueron parte de la reclamación previa presentada ante la autoridad de control, esto es los responsables del tratamiento o su representante, los encargados del tratamiento o su representante.

3. Derechos tutelados

Como esta acción de tutela se interpone respecto de una decisión de una autoridad de control que no se ha pronunciado o lo hecho en referencia a si se ha infringido o no el RGPD, se considera que los derechos tutelados son aquellos reconocidos en los artículos 12 al 22 y el 34 del RGPD.

4. Procedencia

Todo interesado tendrá derecho a presentar solicitar la tutela judicial efectiva en caso de que la autoridad de control competente no dé curso a una reclamación o la autoridad de control que haya dictado una decisión jurídicamente vinculante niegue o desestime total o parcialmente la reclamación previa, o no actúe cuando sea necesario para proteger los derechos del interesado, o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada en virtud del artículo 77.

Adicionalmente, conforme lo dispuesto en el artículo 58 del RGPD, estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, el ejercicio de los poderes de investigación, correctivos, de autorización y colectivos que realice la autoridad de control de un Estado miembro.

El derecho a la tutela judicial efectiva no procede si las medidas adoptadas no son jurídicamente vinculantes, como los dictámenes publicados o el asesoramiento facilitado por ellas (considerando [143], RGPD).

La presentación de la tutela judicial efectiva puede realizarse sin perjuicio de que se haya interpuesto otro recurso administrativo o extrajudicial.

5. Procedimiento

La acción de tutela deberá ejercitarse ante los tribunales del Estado miembro en que esté establecida la autoridad de control, y tramitarse con arreglo al Derecho procesal de dicho Estado miembro, conforme el artículo 78 y el considerando (143) del RGPD.

Cuando la acción de tutela ha sido presentada en contra de una decisión de una autoridad de control que basó su postura en un dictamen o una decisión del Comité, emitida a través del marco del mecanismo de coherencia, la autoridad de control remitirá al tribunal dicho dictamen o decisión.

Además, de conformidad con el considerando (143) del RGPD, toda persona física o jurídica interesada, responsable o encargada, si una decisión del Comité le afecta directa e individualmente, tiene derecho a interponer ante el Tribunal de Justicia el recurso de anulación de decisiones del Comité. Asimismo, podrá interponer este recurso ante las autoridades de control que son destinatarias de dichas decisiones, las cuales deberán darlas a conocer en el plazo de dos meses a partir del momento en que les fueron notificadas.

La autoridad de control facilitará la presentación de reclamaciones mediante medidas como un formulario de reclamaciones físico o electrónico (considerando [141], RGPD).

La tutela judicial efectiva constituye una garantía procesal y un mecanismo de respeto de las garantías procesales adecuadas que se presenta para controlar el ejercicio de los poderes de una autoridad de control (art. 58, num. 4).

En el caso de pendencia deberá aplicarse lo previamente analizado en el acápite anterior y que consta en el artículo 81 del RGPD.

> Conforme el considerando (141) del RGPD, si el asunto requiere una mayor investigación o coordinación con otra autoridad de control, se debe facilitar información intermedia al interesado.

6.9.4 Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento

El artículo 79 del RGPD establece el derecho a la tutela judicial efectiva contra el responsable o encargado del tratamiento, para que este, por sí mismo permita el acceso, modifique, suprima, o en general adapte su comportamiento a las disposiciones contenidas en el RGPD.

Es decir, este derecho consiste en la posibilidad de un titular de datos de solicitar la intervención de un juez para resolver situaciones que el responsable o encargado de tratamiento no ha corregido.

Ahora bien, son los jueces quienes tienen un rol fundamental como garantes de derechos, ya que a través de los:

> Principios y tutela judicial que son especialmente importantes en un contexto en el que cada día se aprecia que la protección de datos debe extenderse a nuevos ámbitos –las telecomunicaciones, la videovigilancia, los servicios de la llamada sociedad de la información, el mundo de Internet– y a nuevos peligros, como los que pueden deparar las llamadas etiquetas inteligentes, los chips incorporados a personas, los brazaletes electrónicos, el uso de datos biométricos como mecanismos de seguridad en la identificación de individuos, extremos todos ellos considerados en la Relazione que en 2003 el Garante italiano para la protección de datos personales, Stefano Rodotá, elevó al Presidente de la República, en la que reflexiona sobre la necesidad de dar una respuesta en términos de tutela del derecho fundamental a los efectos potencialmente nocivos que derivan del innegable progreso tecnológico. En estos casos, en tanto se diseñan y aprueban las normas necesarias para prevenirlos o impedirlos, es en la aplicación judicial de los principios en donde residirá una de las principales líneas de defensa.[755]

Como vemos, mientras que el desarrollo tecnológico va a un ritmo acelerado, la normativa legal que regula de forma preventiva y reactiva su uso inadecuado, tiene procesos de promulgación muy lentos. Por ello, son las autoridades de control junto con los jueces, los responsables de conocer y

[755] P. LUCAS MURILLO DE LA CUEVA, "El derecho a la autodeterminación informativa y la protección de datos personales", *Azpicuelta Cuadernos de Derecho,* 20, (2008): 58, accedido el 16 de noviembre de 2019 https://core.ac.uk/download/pdf/11501784.pdf

dimensionar el derecho a la protección de datos personales para que de producirse una transgresión puedan ser el primer bastión de defensa de los derechos de las personas. Todo lo cual constituye un reto, sobre todo, debido a la necesidad de formación especializada de los jueces, quienes deben comprender la tecnología, así como los derechos fundamentales en riesgo. Ya que, sus decisiones servirán de jurisprudencia orientadora que responde a las problemáticas tecnológicas y sociales, a la vulneración de los datos personales, pero también al libre flujo informacional que permiten el progreso económico y social de una sociedad. Por ello, los jueces deberán resolver estos litigios, a la luz de los principios y derechos digitales.

A continuación se analizarán los elementos básicos que deben determinarse para la vigencia de este derecho subjetivo:

1. *Sujeto activo*

Se considera sujeto activo a todo interesado que considere que, en el tratamiento de sus datos personales, sus derechos han sido transgredidos porque no se ha respetado lo previsto en el Reglamento.

Tal como se señaló en líneas precedentes, para que se inste la tutela judicial efectiva contra el responsable o el interesado, cabe la designación de un representante que será una entidad, organización o asociación sin ánimo de lucro dedicada a la protección de los datos personales. Es este mismo sentido, cualquier Estado miembro puede disponer directamente que alguna de estas organizaciones realice la presentación de la mencionada tutela (art. 80 y considerando [142], RGPD).

2. *Sujetos pasivos u obligados*

Serán sujetos pasivos u obligados aquellos que realizan por su propia cuenta o por cuenta de otros el tratamiento de datos personales del interesado, estos son: el responsable del tratamiento o su representante y el encargado del tratamiento o su representante.

3. *Derechos tutelados*

Todo interesado tendrá derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento cuando considere que cualquiera de estos, en el tratamiento de sus datos personales, ha vulnerado los derechos recogidos en el citado reglamento.

Como esta acción de tutela se interpone respecto de una decisión de una autoridad de control, que previamente se ha pronunciado sobre si el tratamiento de datos personales infringió el RGPD, se considera que los derechos tutelados son aquellos reconocidos en los artículos 12 al 22 y el 34 del RGPD.

4. Procedencia

Todo interesado tendrá derecho a presentar tutela judicial efectiva aunque se haya interpuesto otro recurso administrativo o extrajudicial disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control previsto en el artículo 77 del RGPD.

5. Procedimiento

La acción de tutela judicial efectiva contra un responsable o encargado del tratamiento deberá ejercitarse ante los tribunales del Estado miembro en el cual el responsable o encargado tenga un establecimiento.

Alternativamente, esta acción de tutela judicial efectiva podrá ejercitarse ante los tribunales del Estado miembro en cual el interesado tenga su residencia habitual.

En el caso de un responsable o encargado que sea una autoridad pública que actúe en ejercicio de sus poderes públicos, la acción de tutela judicial efectiva deberá presentarse ante los tribunales del Estado miembro de donde provenga dicha autoridad pública.

En el caso de dependencia deberá aplicarse lo previamente analizado en el acápite anterior y que consta en el artículo 81 del RGPD.

6.9.5 Derecho a indemnización y responsabilidad

Otra de las reclamaciones que puede realizar el interesado es aquella que consta en el artículo 82 del RGPD, mediante la cual se solicita del responsable la indemnización de los daños y perjuicios causados por las transgresiones a los derechos del titular por el indebido tratamiento de sus datos personales; para un análisis pormenorizado se estudiarán las siguientes categorías:

1. *Sujeto activo:*

Se considera sujeto activo a toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del Reglamento.

El considerando (142) del RGPD establece que una entidad, organización o asociación no puede estar autorizada a reclamar una indemnización en nombre de un interesado aunque el interesado haya emitido mandato a su favor.

2. *Sujeto pasivo*

Se considera sujeto pasivo al responsable que ha participado en la operación de tratamiento que ha producido los daños y perjuicios por no haber respetado lo dispuesto en el Reglamento.

También se considerará sujeto pasivo al encargado que ha participado en el tratamiento que ha producido daños y perjuicios por no haber cumplido con las obligaciones propias de estos encargados previstas en el RGPD, o cuando haya actuado al margen o en contra de las instrucciones legales del responsable.

El responsable o encargado del tratamiento estará exento de responsabilidad si demuestra que no son responsables del hecho que causó los daños y perjuicios, nexo causal.

Por otro lado, rige el principio de responsabilidad solidaria, por cuanto cada responsable o encargado, cuando hayan participado más de uno en la misma operación de tratamiento de datos, será responsable de cualquier daño o perjuicio causado, a fin de garantizar la indemnización efectiva del interesado, sin perjuicio de los derechos posteriores de solicitarse la cuota de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados (art. 82, num. 5, RGPD).

3. *Derechos tutelados*

Todos los derechos reconocidos en el RGPD que debido a su vulneración han producido daños materiales o inmateriales a su titular y que puedan ser avaluados a título de indemnización.

4. *Procedencia*

Tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

5. *Procedimiento*

Las acciones judiciales para exigir la indemnización se presentarán ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento o, en su caso, ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual; menos cuando el responsable o el encargado es una autoridad pública que actúe en ejercicio de sus poderes públicos (art. 79, apdo. 2, RGDP).

6.10 Institucionalidad de protección

Para la efectiva vigencia de los derechos y garantías previstos en el RGPD se ha previsto una institucionalidad de protección dividida jerárquicamente en función de sus atribuciones y competencias con la finalidad de motivar el cumplimiento del Reglamento, prevenir posibles transgresiones, vigilar y sancionar su incumplimiento dentro de cada Estado miembro, y además el establecimiento uniforme y coherente dentro del espacio europeo.

Para el análisis de este sistema, se estudiarán tanto las distintas instituciones que se han creado en cada Estado miembro como los organismos asociados a la Unión Europea que en virtud del RGPD tienen nuevas competencias y funciones; estos son: la o las autoridades de control, incluida la autoridad de control principal, el Comité Europeo de Protección de Datos y la Comisión Europea.

6.10.1 Autoridad de control

El artículo 51 del RGPD establece que cada Estado miembro, en su territorio, establecerá una o varias autoridades de control para supervisar la aplicación del Reglamento y de forma coherente en toda la Unión, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento de sus datos personales y al mismo tiempo facilitar el libre flujo informacional en la Unión.

Cuando se hayan establecido varias autoridades de control en un Estado, se designará la autoridad de control que representará a dichas autoridades en el Comité, a la cual se denominará autoridad de control principal. Y además, se establecerá la forma en la que se dará cumplimiento al mecanismo de coherencia constante en el artículo 63 del RGPD.

1. Clases de independencia que debe ostentar la autoridad de control

El RGPD establece como presupuesto primigenio la independencia de la autoridad de control, por ello antes incluso de determinar las competencias, funcionamiento, poderes y otros procedimientos de funcionamiento, ha hecho especial mención en el artículo 52 del citado Reglamento a esta cuestión. De manera que se vuelve condición inexorable, presupuesto ineludible en la designación de una o más autoridades de control en un país miembro de la Unión.

Como antecedente de lo expresado, figura en la sentencia Comisión/Alemania resuelta y emitida el 9 de marzo de 2010 por el Tribunal de Justicia de la Unión Europea, en la cual se señala respecto del artículo 28 de la Directiva 95/46 que "las autoridades de control en materia de protección de datos personales han de disfrutar de una independencia que les permita ejercer sus funciones sin influencia externa, y además que «deben estar a resguardo de toda influencia externa, ejercida directa o indirectamente, que pueda orientar sus decisiones»".[756]

El considerando (118) del RGPD señala que la independencia de las autoridades de control no debe significar que puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial.

Esta norma citada, además especifica los tipos de independencia que deben estar garantizadas para que se viabilice el trabajo imparcial y técnico de estos organismos de control. Así pues, no se trata de un simple enunciado retórico, sino que intenta escrutar todas las posibles formas de afectación estableciendo prohibiciones expresas o condiciones básicas que garanticen en su conjunto la independencia de funcionarios, procesos, autoridades; en suma, de la institucionalidad concreta que controla la protección de datos personales en cada Estado miembro.

En ese sentido se han previsto las siguientes categorías de independencia:

a) Independencia de cada autoridad de control

Cada autoridad de control actuará con total independencia en el desempeño de sus funciones y en el ejercicio de los poderes de investigación, correctivos, de autorización y consultivos, denominados en su conjunto poderes públicos.

[756] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C518/07, en el caso: Comisión/Alemania], 2010, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/liste.jsf?language=es&num=C-518/07

b) Independencia del miembro o de los miembros de cada autoridad de control

Se garantizará que el miembro o los miembros de cada autoridad de control no estén sujetos a influencia externa, ya sea directa o indirecta; además, no se solicitará ni admitirá ninguna forma de instrucción, en el desempeño de sus funciones y en el ejercicio de sus poderes públicos.

c) Incompatibilidad de actividades de los miembros o miembros

El miembro o los miembros de cada autoridad de control se abstendrán de realizar de cualquier acción pública o privada que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no. En este mismo sentido, consta el considerando (121) del RGPD.

d) Independencia de recursos humanos, técnicos y financieros

Otra de las formas de independencia que garantiza imparcialidad en las decisiones es la relativa a la autonomía de los recursos humanos, técnicos y financieros. De modo que cada Estado miembro debe garantizar que cada autoridad de control disponga en todo momento de locales e infraestructuras necesarias para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, y de aquellas facultades previstas en el marco de la asistencia mutua, la cooperación y la participación en el Comité.

e) Independencia del control financiero

Las autoridades de control estarán sujetas a un control financiero que no afecte a su independencia. Además, cada Estado miembro garantizará que cada autoridad de control disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional. En el mismo sentido, el considerando (120) del RGPD.

f) Libertad en el escogimiento del personal

Para garantizar la independencia también es necesario que cada autoridad de control pueda elegir y disponer de su propio personal, de manera que esta sea su autoridad exclusiva.

La Disposición transitoria primera de la LOPDGDD señala que lo relativo a la designación, procedimiento y mandato sobre los miembros de la Agencia de Protección de Datos Personales, que consta en la citada Ley y en l RGPD, se aplicará una vez expire el mandato de quien ostente la condición de Director de la Agencia Española de Protección de Datos. La redacción de esta norma cumple con los criterios que constan dispuesto en el TJUE en su sentencia de 8 de abril de 2014 (asunto c-288/12) que señalan:

> En esta sentencia se analiza la cuestión de si se incumplen las obligaciones que incumben a un Estado miembro en virtud de la Directiva 95/46/CE, en relación con la independencia de la autoridad de control, en este caso Hungría, al poner fin antes de tiempo a su mandato. (…) Y añade que «para apreciar el fundamento del presente recurso es necesario analizar si, como sostiene la Comisión, la exigencia, contemplada en el artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46, según la cual debe garantizarse que cada autoridad de control ejerza con total independencia las funciones que le son atribuidas, implica que el Estado miembro de que se trate está obligado a respetar la duración del mandato de tal autoridad hasta que llegue a su término inicialmente previsto» (Apartado 50). (…) Y a partir de estas consideraciones concluye que «Pues bien, si cada Estado miembro tuviera la posibilidad de poner fin al mandato de una autoridad de control antes de que éste llegue al término inicialmente previsto sin respetar las normas y las garantías establecidas previamente en tal sentido por la legislación aplicable, la amenaza de tal terminación anticipada que en tal caso planearía sobre esa autoridad durante todo su mandato podría generar una forma de obediencia de ésta al poder político incompatible con dicha exigencia de independencia (...). Esta conclusión es también cierta en el caso de que la finalización del mandato antes de tiempo obedezca a una reestructuración o a un cambio de modelo, los cuales deben organizarse de modo que respeten las exigencias de independencia impuestas por la legislación aplicable.[757]

De lo señalado, aun cuando ha entrado en vigencia el RGPD y la LOPDGDD, deberá respetarse el tiempo de designación de las autoridades de la AEPD dado que el acatamiento del tiempo de designación es fundamental para la garantía de independencia.

Finalmente, la independencia de la autoridad de control también puede manifestarse en otras condiciones impuestas tanto por el RGPD como por la LOPDGDD que, por ejemplo, señala que:

> La garantía de la independencia de la Agencia se completa con la exigencia de que la autoridad se someta al control parlamentario y de la opinión pública. Control asociado a la

[757] J. Rubí Navarrete, "La Agencia Española de Protección de Datos", *Tratado de protección de datos*, Coordinador: A. RALLO LOMBARTE, (Valencia: Tirant lo Blanch on line, 2019)

obligación del RGPD de elaborar un informe anual de actividad que debe transmitirse, entre otros, al Parlamento nacional y ponerse a disposición del público (art. 59). [758]

2. Condiciones generales aplicables a los miembros de la autoridad de control

El considerando (117) del RGPD señala que constituye un elemento esencial de la protección, el establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia; así como, que los Estados miembros establezcan más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa.

Un precedente de lo anotado, se destaca en la sentencia ya citada de la Comisión/Alemania resuelta y emitida el 9 de marzo de 2010 por el Tribunal de Justicia de la Unión Europea, en el cual se indica que "la creación en cada uno de los Estados miembros de autoridades de control independientes constituye un elemento esencial del respeto a la protección de las personas en lo que respecta al tratamiento de datos personales". [759]

En aquel contexto, el artículo 53 del RGPD señala las condiciones generales aplicables a los miembros de cada autoridad de control en garantía de su independencia y de la imparcialidad en la toma de decisiones:

a) *Designación y nombramiento transparente*: Los Estados miembros dispondrán que sus autoridades de control sean nombrados mediante un procedimiento transparente por: — su Parlamento, — su Gobierno, — su Jefe de Estado, o — un organismo independiente encargado del nombramiento en virtud del derecho de los Estados miembros.

b) *Requisitos:* Los miembros de la autoridad de control poseerán obligatoriamente de la titulación, la experiencia y las aptitudes relacionadas con la protección de datos personales para el ejercicio de sus competencias, funciones y poderes públicos.

c) *Terminación de funciones:* Los miembros de la autoridad de control darán por concluidas sus funciones por terminación del mandato, dimisión o jubilación obligatoria, de ser el caso.

[758] Ibíd.
[759] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C518/07, en el caso: Comisión/Alemania], 2010, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/liste.jsf?language=es&num=C-518/07

d) *Destitución:* Podrá producirse la destitución de un miembro en caso de conducta irregular grave o incumplimiento de las condiciones propias de la designación.

3. Normas relativas al establecimiento de la autoridad de control

El artículo 54 señala la obligación de cada Estado miembro de establecer por ley todos los elementos que se indican a continuación, relativos al establecimiento y funcionamiento de la autoridad de control en un Estado miembro, para que esta efectivamente pueda realizar su trabajo con independencia, imparcialidad, eficiencia y apego a lo dispuesto en el RGPD.

a) *El establecimiento de la autoridad de control*: Debe instaurarse por ley la forma de establecimiento de cada autoridad de control.
b) *El proceso de designación de los miembros de la autoridad de control:* Que incluirá los requisitos, cualificaciones, condiciones de idoneidad intelectual y personal necesarias; así como, las normas y procedimientos para el nombramiento.
c) *La duración de las funciones y las posibilidades de su renovación en el cargo:* Se deberá establecer la duración del mandato del miembro o los miembros de cada autoridad de control, que no podrá ser inferior a cuatro años. Además de la posibilidad de que el mandato sea renovable, determinando los requisitos de alternabilidad como el número de veces que podrá renovarse y en qué condiciones.
d) *Incompatibilidades y prohibiciones:* Prohibiciones sobre acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, incluidos convenios de confidencialidad, el deber de secreto de sus funciones y en especial de la información recibida de personas físicas en relación con infracciones, y las normas que rigen el cese en el empleo.
e) *Diferencias entre autoridad de control y autoridades de control interesadas*: El artículo 4, numeral 21) del RGPD define a la autoridad de control como aquella autoridad pública independiente establecida por un Estado; mientras que la autoridad de control interesada es aquella a la que afecta el tratamiento de datos personales debido a que:

    a. el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;
    b. los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento; o
    c. se ha presentado una reclamación ante esa autoridad de control.

La nueva LOPDGDD española ha determinado en sus artículos 48, 49 y 50 un cambio en la institucionalidad de protección, ya que reconoce la figura de un Presidente con amplios poderes y

atribuciones y además una autoridad adjunta, a quien se podrá delegar las funciones del titular, o de ser el caso actuar como sustituto:

> […] sobre la designación de los miembros de la AEPD, la Ley (art. 48) modifica su composición pasando de un Director que asume la totalidad de las competencias y funciones atribuidas a la Agencia a una Presidencia. Y la creación de una figura auxiliar de la misma constituida por un Adjunto al que se aplica, también, el procedimiento de designación de la Presidencia que se ha descrito anteriormente".[760]

Pero además, establece la creación de un Consejo Consultivo que tendrá la función de asesorar a la Presidencia de la Agencia Española de Protección de Datos cuyas decisiones serán meramente orientativas, por cuanto no tienen efecto vinculante.

4. Competencias de las autoridades de control y de la autoridad de control principal

En el considerando (122) y en los artículos 55 y 56 constan descritas las competencias atribuibles a las autoridades de control, en especial a la autoridad de control principal con miras a garantizar los derechos humanos en el tratamiento de los datos personales de los interesados en el espacio europeo.

a) Competencias generales de las autoridades de control:

De conformidad con el artículo 55 del RGPD, cada autoridad de control será competente para:

a. Desempeñar las funciones y poderes públicos que consten en la normativa de cada país y del RGPD en el territorio de su Estado miembro.
b. Cuando el tratamiento sea efectuado por autoridades públicas para el cumplimiento de una obligación legal o de una misión realizada en interés o ejercicio de poderes públicos, será competente la autoridad de control del Estado miembro de que se trate y no será competente la autoridad de control principal.
c. No serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.

b) Competencias de la autoridad de control principal

[760] J. RUBÍ NAVARRETE, *op.cit.*

El artículo 56 del RGPD establece las competencias específicas de la autoridad de control principal que serán:

a. Desempeñar las funciones y poderes públicos que consten en la normativa de cada país y del RGPD en el territorio de su Estado miembro.
b. Realizar funciones de único interlocutor respecto del tratamiento transfronterizo de datos realizado por el responsable o del encargado, en el establecimiento principal o en el único establecimiento de estos (en este mismo sentido el considerando (124), RGPD).
c. Tratar una reclamación o una posible infracción del Reglamento, cuando el establecimiento esté situado en su Estado miembro o afecte de manera sustancial a interesados en su Estado miembro.
d. La autoridad de control informará, sin dilación alguna, de una reclamación presentada o una posible infracción del Reglamento a la autoridad de control principal.

i. La autoridad de control en el plazo de tres semanas después de haber sido informada decidirá si tratará o no el caso de conformidad con el procedimiento de mecanismo de coherencia (art. 60, RGPD
ii. La autoridad de control deberá revisar si existe un establecimiento del responsable o encargado del tratamiento en el Estado miembro de la autoridad de control que le haya informado.
iii. La autoridad de control que haya informado a la autoridad de control principal podrá presentarle un proyecto de decisión.
iv. En caso de que la autoridad de control principal decida no tratar el caso, la autoridad de control que le haya informado lo tratará como asistencia mutua o de operaciones conjuntas, al tenor de los artículos 61 y 62 del RGPD.

Conforme el artículo 44 numeral 2 de la LOPDGDD, la Agencia Española de Protección de Datos será la representante común de las autoridades de protección de datos de España ante el Comité Europeo de Protección de Datos.

5. Funciones de cada autoridad de control

Tal como señala el artículo 57 del RGPD, cada autoridad de control incluida la principal dentro de su territorio, tendrá las siguientes funciones, sin perjuicio de otras establecidas por el mismo reglamento.

a) Sobre el cumplimiento del RGPD

a. Verificar que se aplique y controle la forma de aplicación del RGPD.

b. Llevar a cabo investigaciones sobre la aplicación del Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública.
c. Hacer seguimiento del desarrollo de tecnologías de la información y la comunicación, y de prácticas comerciales que pudieran representar un riesgo en la protección de datos personales.
d. Llevar registros internos de las infracciones y de las medidas correctivas impuestas de conformidad con el artículo 58, apartado 2.
e. Desempeñar cualquier otra función relacionada con la protección de los datos personales.

b) Sobre promoción de derechos

Promover la sensibilización y comprensión del público sobre los riesgos, normas, garantías y derechos, en especial dirigido a niños, y de los responsables y encargados respecto de sus obligaciones, incluidas las microempresas y las pequeñas y medianas empresas, al tenor del considerando (132) del RGPD.

c) Sobre asesoramiento y cooperación

a. Asesorar sobre medidas legislativas y administrativas que puedan implementarse.
b. Cooperar con las autoridades de control de otros Estados miembros respecto de facilitar información para el ejercicio de derechos y en especial compartiendo información, con otras autoridades de control.
c. |Prestar asistencia mutua con otras autoridades de control con el fin de garantizar la coherencia en la aplicación y ejecución del RGDP.
d. Ofrecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2.
e. Contribuir a las actividades del Comité.

d) Sobre reclamaciones

a. Investigar, procesar y resolver las reclamaciones presentadas por un interesado o por un organismo, organización o asociación (ver acápite 6.8 b) del presente trabajo de investigación.
   Al respecto, en el caso Google Spain y Google, previamente citado y en virtud del artículo 28, apartados 3 y 4, de la Directiva 95/46, el Tribunal de Justicia de la Unión Europea destaca "que toda autoridad de control entenderá de las solicitudes de cualquier persona relativas a la protección de sus derechos y libertades en relación con el tratamiento de datos personales y que dispone de poderes de investigación y de poderes efectivos de intervención, que le

permiten, en particular, ordenar el bloqueo, la supresión o la destrucción de datos, o prohibir provisional o definitivamente un tratamiento".[761]

b. Facilitar reclamaciones a los interesados mediante formularios físicos o virtuales.
c. Previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos.
d. Gratuidad para el interesado del desempeño de las funciones de cada autoridad de control y del delegado de protección de datos. Se admitirá una tasa razonable basada en los costes administrativos o la negativa de la solicitud si esta es manifiestamente infundada o excesiva, especialmente debido a su carácter repetitivo, pero la carga de la prueba de estas aseveraciones estará en manos de la autoridad de control.

e) Sobre condiciones uniformes de ejecución del RGPD

El considerado (167) del RGPD señala que se conferirá a la Comisión Europea de aquellas competencias que le faculten establecer condiciones uniformes de ejecución. Aunque esta referencia, hacen alusión a competencias de la Comisión, no se limita a este organismo. Pues, debe ser entendida como aquellos medios o mecanismos que de producirse permiten cumplir con el fin de homogenizar la aplicación del RGPD. Por ejemplo, la adopción de medidas específicas para que microempresas y pequeñas y medianas empresas cumplan con las disposiciones el RGPD.

Entre los mecanismos que permiten el establecimiento de condiciones uniformes de ejecución del RGPD constan las siguientes:

a. Adoptar cláusulas contractuales tipo, tanto para cuando existe acto o contrato que establezca la existencia de una relación jurídica (art. 28, num. 8), como aquellas aprobadas por la Comisión para el procedimiento de examen establecido en el artículo 93, numeral 2 del RGPD.
b. Autorizar las cláusulas contractuales y disposiciones a que se refiere el artículo 46, apartado 3 relativas a datos que se entregan a terceros países o entre autoridades públicas.
c. Aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.
d. Elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, en virtud del artículo 35, apartado 4 del RGPD.
e. Fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos y llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas.

[761] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C-131/12, en el caso: Google Spain y Google], 2014, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES.

f. Promover la elaboración de códigos de conducta, dictaminar y aprobar códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartados 1 y 5.
g. Elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta.
h. Efectuar la acreditación de organismos de supervisión de los códigos de conducta.

La Agencia Española de Protección de Datos tendrá la función de supervisar la aplicación del RGPD y de la LOPDGDD, conforme el artículo 47. Debido a que el ámbito de aplicación de la norma española incluye la protección de los derechos digitales, la competencia de la Agencia Española de Protección de Datos se amplía a dichos derechos, para los cuales podrá usarse la institucionalidad, los mecanismos, poderes y demás herramientas disponibles.

6. Poderes de cada autoridad de control

El artículo 58 establece los siguientes poderes que cada autoridad de control dispondrá para el ejercicio de las funciones a su cargo:

a) Poderes de investigación

La citada norma establece que los órganos de control tendrán los siguientes poderes investigativos:

a. Ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones, incluido el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones.
b. Llevar a cabo investigaciones en forma de auditorías de protección de datos.
c. Revisar certificaciones expedidas previamente emitidas.
d. Notificar al responsable o al encargado del tratamiento las presuntas infracciones al RGPD.
e. Obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos.

b) *Poderes correctivos*

Cada autoridad de control dispondrá de los siguientes poderes correctivos:

a. Sancionar a todo responsable o encargado del tratamiento con una advertencia o con apercibimiento, cuando las operaciones de tratamiento previstas puedan o hayan infringido el RGPD, respectivamente.
b. Ordenar al responsable o encargado del tratamiento o sus respectivos representantes que:

    i. atiendan las solicitudes de ejercicio de los derechos del interesado, incluida la rectificación o supresión de datos personales o la limitación de tratamiento y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales;
    ii. se ajusten a las disposiciones del Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;
    iii. se comunique al interesado las violaciones de la seguridad de los datos personales;
    iv. se suspenda los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional;
    v. se ejecute una limitación temporal o definitiva del tratamiento, previamente impuesta en la que conste una prohibición.

c. Retirar una certificación u ordenar al organismo de certificación que retire una certificación o que no se emita una certificación si no se cumplen o si dejan de cumplirse los requisitos para la certificación.
d. Imponer una multa administrativa además o en lugar de las medidas correctivas mencionadas, de ser el caso.

c) *Poderes de autorización y consultivos*

Cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación:

a. Emitir dictámenes de oficio o a petición de parte sobre protección de los datos personales, para el Parlamento nacional, el Gobierno del Estado miembro u otras instituciones y organismos, así como al público.
b. Asesorar al responsable del tratamiento conforme al procedimiento de consulta previa en casos de evaluaciones de impacto negativas, del artículo 36.
c. Autorizar el tratamiento de datos para el cumplimiento de una misión realizada de interés público, en particular el tratamiento en relación con la protección social y la salud pública, de conformidad con la normativa de cada Estado miembro.
d. Emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 40.
e. Adoptar cláusulas contractuales tipo de protección, tanto para cuando existe un acto o contrato que establezca la existencia de una relación jurídica (art. 28, num. 8) como aquellas aprobadas por la Comisión para el procedimiento de examen establecido en el artículo 93, numeral 2 del RGPD.

f. Autorizar las cláusulas contractuales para la transferencia de datos mediante garantías adecuadas en un tercer país (art. 46, apdo. 3, lit. a, RGPD).
g. Autorizar los acuerdos administrativos para la transferencia de datos mediante garantías adecuadas en un tercer país, artículo 46, apartado 3, letra b).
h. Aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.
i. Acreditar los organismos de certificación con arreglo al artículo 43 y expedir certificaciones y aprobar criterios de certificación, artículo 42, apartado 5.

d) *Características comunes a los poderes de la autoridad de control*

a. Conforme el artículo 58 del RGPD, cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para:

i. Poner en conocimiento de las autoridades judiciales las infracciones del Reglamento;
ii. iniciar o ejercitar acciones judiciales, con el fin de hacer cumplir lo dispuesto en el reglamento;
iii. tener otros poderes públicos adicionales a los investigativos, correctivos y de autorización y consultivos descritos anteriormente.

b. Cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de los tipos de medidas correctivas adoptadas como advertencias, apercibimiento y órdenes, de conformidad con el artículo 58, apartado 2. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las demás autoridades y se pondrán a disposición del público, de la Comisión y del Comité (art. 59).

c. Estarán sujetos a garantías adecuadas, incluida la tutela judicial efectiva y el respeto de las garantías procesales, el ejercicio de los poderes de investigación, correctivos, de autorización que realice la autoridad de control de un Estado miembro (art. 58, RGPD).

Cabe mencionar que como antecedente, el Tribunal de Justicia de la Unión Europea dispuso en el caso Comisión/Alemania, con sentencia emitida el 9 de marzo de 2010, y en conformidad con el artículo 28, apartado 6, de la Directiva 95/46, que “las autoridades nacionales cooperarán entre sí, y, llegado el caso, incluso podrán ser instadas a ejercer sus poderes por una autoridad de otro Estado miembro”.

7. Mecanismos de cooperación y coherencia entre autoridad de control principal y otras autoridades de control

El considerando (119) del RGPD estipula que si un Estado miembro establece varias autoridades de control, deben existir mecanismos de participación efectiva entre autoridades de control. Cada Estado miembro debe designar a la autoridad de control que actuará como punto de contacto único para agilitar las interacciones con otras autoridades de control, con el Comité y la Comisión.

De conformidad con el artículo 60, para la coherencia de las decisiones y actuaciones en el marco de las competencias, funciones y poderes públicos de las autoridades de control principal y de otras autoridades de control interesadas, se han previsto los mecanismos de cooperación y coherencia en la búsqueda obligatoria que deben hacer las instituciones por llegar a un consenso; dichos mecanismos de cooperación y coherencia son:

a) *Intercambio de información pertinente*

La autoridad de control principal y las autoridades de control interesadas intercambiarán toda información pertinente, de forma recíproca y por medios electrónicos, utilizando un formulario normalizado, que facilite el ejercicio de las funciones de cada uno y que además viabilice llegar a un consenso.

b) *Cooperación para realizar investigaciones o supervisar aplicación de medidas*

La autoridad de control principal de manera general y en especial para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro:

a. Cooperará con las demás autoridades de control interesadas en búsqueda del consenso.
b. Podrá solicitar en cualquier momento a otras autoridades de control presten asistencia mutua (art. 61, RGPD).
c. Podrá llevar a cabo operaciones conjuntas (art. 62, RGPD).

c) *Decisión*

De conformidad con el artículo 60 del RGDP, respecto de un tema puesto en conocimiento de una autoridad de control principal por parte de una parte interesada, existe la obligación de que esta autoridad dicte una decisión que satisfaga las inquietudes presentadas. La decisión deberá tomarse sin dilación alguna.

La decisión será construida mediante un proceso de diálogo entre entidades de control, de modo que si alguna no está de acuerdo con el proyecto remitido puede presentar

objeciones, que de existir serán sometidas al mecanismo de coherencia contemplado en el artículo 63; esto es para decisión del Comité.

En caso de que ninguna autoridad de control interesada haya presentado objeciones o que habiéndose presentado, la autoridad de control se haya allanado a ellas, se volverá a transmitir la decisión a las otras autoridades; en el caso de no presentarse nuevas objeciones, se considerará que las partes están de acuerdo.

La autoridad de control principal y la que recibió la petición adoptará y notificará la decisión, tanto al reclamante como al establecimiento principal o al establecimiento único del responsable o el encargado del tratamiento, e informará de la decisión a las autoridades de control interesadas y al Comité, incluyendo un resumen de los hechos pertinentes y la motivación.

8. Procedimiento de urgencia

En circunstancias excepcionales, cuando una autoridad de control interesada tenga motivos para considerar que es urgente intervenir para proteger los intereses de los interesados, se aplicará el procedimiento de urgencia a que se refiere el artículo 66 del RGDP.

Si una autoridad de control no resuelve la adopción de un procedimiento de emergencia en el plazo de un mes a partir de la recepción de la solicitud, la autoridad de control requirente podrá adoptar una medida provisional en el territorio de su Estado miembro. En ese caso, se supondrá que existe la necesidad urgente contemplada en el artículo 66, apartado 1, que exige una decisión urgente y vinculante del Comité en virtud del artículo 66, apartado 2 del RGDP.

Cuando se prevea una operación conjunta y una autoridad de control no cumpla en el plazo de un mes con la obligación establecida en el apartado 2, segunda frase, del presente artículo, las demás autoridades de control podrán adoptar una medida provisional en el territorio de su Estado miembro de conformidad con el artículo 55. En ese caso, se presumirá la existencia de una necesidad urgente a tenor del artículo 66, apartado 1, y se requerirá dictamen o decisión vinculante urgente del Comité, en virtud del artículo 66, apartado 2 del RGDP.

9. Asistencia mutua

El artículo 61 del RGDP establece los mecanismos de asistencia mutua que permiten adoptar medidas oportunas para responder a las solicitudes entre autoridad de control, sin dilación indebida y a más tardar en el plazo de un mes contados desde la presentación de la solicitud.

La asistencia mutua de manera general se aplica a:

a) Facilitar información útil, en su mayoría en formato electrónico y normalizado, en particular, la transmisión de información pertinente sobre el desarrollo de una investigación. La información que se intercambie se utilizará únicamente para el fin para el que haya sido solicitada.
b) Tomar medidas de control para asegurar una efectiva cooperación entre ellas, como las solicitudes para llevar a cabo autorizaciones y consultas previas, inspecciones e investigaciones.

La autoridad de control requerida no podrá negarse a responder a una solicitud, a menos que:

a) no sea competente en relación con el objeto de la solicitud o con las medidas cuya ejecución se solicita;
b) De contestar la solicitud, se infrinja el RGPD o la norma interna del Estado miembro.

Pero aunque su respuesta fuera negativa explicará los motivos de su negativa a responder.

La autoridad de control requerida está en la obligación de informar a la autoridad de control requirente los resultados obtenidos o, en su caso, los progresos o las medidas adoptadas para responder a su solicitud. No cobrará tasa alguna, pero podrá convenir normas de indemnización recíproca por gastos específicos derivados de la prestación en circunstancias excepcionales.

10. Actos de ejecución

Los actos de ejecución son mecanismos que facilitan el examen al que se refiere el artículo 93, apartado 2 del RGPD.

En ese sentido, la Comisión podrá, mediante estos actos de ejecución, especificar:

a) el formato;
b) los procedimientos de asistencia mutua;
c) las modalidades del intercambio de información por medios electrónicos entre las autoridades de control y entre las autoridades de control y el Comité;
d) el formato normalizado de intercambio.

11. Operaciones conjuntas de las autoridades de control

El artículo 62 del RGPD estipula condiciones y procedimientos para establecer operaciones conjuntas de las autoridades de control, al tenor de los siguientes criterios:

a) Las operaciones conjuntas incluirán investigaciones y medidas de ejecución conjuntas, en las que participen personal de las autoridades de control de otros Estados miembros.
b) Proceden operaciones conjuntas cuando el responsable o el encargado del tratamiento tiene establecimientos en varios Estados miembros, o es probable que un número significativo de interesados en más de un Estado miembro puedan verse sustancialmente afectados por las operaciones de tratamiento.
c) La utilización de poderes públicos por parte del personal de las autoridades de control de otro Estado miembro distinto a los que tienen competencia, de conformidad con la normativa de cada Estado miembro y el RGPD.

Como antecedente de los mecanismos de cooperación podemos citar el caso Weltimmo, emitido el 1 de octubre de 2015, relativo a la recepción de denuncias sobre el tratamiento de datos por un responsable establecido en otro Estado miembro. Al respecto, el Tribunal de Justicia de la Unión Europea menciona "que corresponde instar, en ejecución de la obligación de *cooperación* que se establece en el artículo 28, apartado 6, de la citada Directiva, a la autoridad de control de ese otro Estado miembro a declarar una eventual infracción de ese Derecho y a imponer sanciones si éste lo permite, basándose, en su caso, en la información que ella le haya remitido".[762]

6.10.2 Comité Europeo de Protección de Datos

En virtud del artículo 29 de la Directiva 95/46/CE se creó el Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, conocido como G29. Que era un órgano consultivo independiente de la Unión Europea conformado por un representantes de cada autoridad de control de cada Estado miembro; de las instituciones comunitarias y de un represente de la Comisión. Entre varias de sus finalidades constaba la de pronunciarse con criterio orientador sobre cuestiones relacionadas con protección de datos y privacidad.

Sus deberes y atribuciones constaban en el artículo 30 de la citada Directiva derogada y en el artículo 15 de la Directiva 2002/58/CE. Se reconoce su importancia, porque ha emitido varios criterios orientadores, incluso su postura de que la Directiva no se aplicaba de forma uniforme en la Unión Europa facilitó la decisión de elevar a nivel de Reglamento la normativa de protección de datos personales. Sin embargo, para muchos el G29:

> […] no era más que uno de los muchos grupos de expertos, de carácter consultivo e independiente, que asesoraban a la Comisión Europea. No obstante, el Grupo fue ganando autoridad e influencia con sus opiniones durante el transcurso de los años, sobre todo en materia de transferencias internacionales de datos. El Grupo tomaba sus decisiones por mayoría simple y tenía por objetivo principal «estudiar toda cuestión

[762] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, [Asunto C230/14, en el caso: Weltimmo], 2015, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/liste.jsf?td=ALL&language=es&jur=C,T,F&num=C-230/14

> relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva con vistas a contribuir a su aplicación homogénea». Su labor se puede considerar bastante exitosa desde la perspectiva de la producción del denominado «*soft law*» en materia de protección de datos, pues muchas de sus opiniones sirvieron para interpretar tanto la Directiva como las normas nacionales de transposición, y algunas fueron citadas por las autoridades nacionales de protección de datos y jueces y tribunales en sus resoluciones. Sin embargo, su dinámica eminentemente gubernamental supuso un lastre importante, pues el Grupo actuaba *de facto* buscando la unanimidad, lo que a menudo restaba contundencia y utilidad a sus opiniones, y su contribución a la aplicación homogénea de las normas nacionales de transposición fue muy escasa. El mejor ejemplo de esta deriva intergubernamental se vio reflejado en la falta de aplicación del artículo 30.2 que disponía que «si el Grupo comprobare la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión».[763]

De esta transcripción, se puede colegir porque el RGPD decidió institucionalizar, a este grupo de expertos, como Organismo de la Unión Europea para que sus actividades no se limiten a la de emisión de *soft law* sino que puedan dictar normativa con efecto vinculante, con la que se garantice la aplicación uniforme del RGPD en todos los países de la Unión.

A partir de la entrada en vigor del RGPD el 25 de mayo de 2018 y por ende de la derogatoria de la Directiva 95/46/CE, el Grupo 29 se elimina y es sustituido por el Consejo Europeo de Protección de Datos, en adelante CEPD.

Antes de su eliminación, el G29 dictó varias directrices y otros documentos sobre varios aspectos del GDPR, para una aplicación consistente en la Unión. El CEPD reconoce 16 informes, pautas, guías o dictámenes elaborados por el G29[764], sin perjuicio de que a futuro pueda realizar revisiones de ser el caso.[765]

---

[763] L. CERVERA NAVAS, "El Comité Europeo de Protección de Datos", *Tratado de protección de datos*, Coordinador: A. RALLO LOMBARTE, (Valencia: Tirant lo Blanch on line, 2019)

[764]

1. Directrices sobre el consentimiento en virtud del Reglamento 2016/679, WP259 rev.01
2. Directrices sobre transparencia en virtud del Reglamento 2016/679, WP260 rev.01
3. Directrices sobre la toma de decisiones y la elaboración de perfiles individuales automatizados a los efectos del Reglamento 2016/679, WP251rev.01
4. Directrices sobre notificación de incumplimiento de datos personales en virtud del Reglamento 2016/679, WP250 rev.01
5. Directrices sobre el derecho a la portabilidad de datos en virtud del Reglamento 2016/679, WP242 rev.01
6. Directrices sobre la evaluación del impacto de la protección de datos (DPIA) y determinar si el procesamiento es "probable que genere un alto riesgo" a los efectos del Reglamento 2016/679, WP248 rev.01
7. Directrices sobre oficiales de protección de datos ('DPO'), WP243 rev.01
8. Pautas para identificar la autoridad supervisora principal de un controlador o procesador, WP244 rev.01
9. Documento de posición sobre las excepciones a la obligación de mantener registros de las actividades de procesamiento de conformidad con el Artículo 30 (5) del RGPD
10. Documento de trabajo que establece un procedimiento de cooperación para la aprobación de "Reglas corporativas vinculantes" para controladores y procesadores bajo el GDPR, WP 263 rev.01
11. Recomendación sobre la Solicitud estándar para la aprobación de las Reglas corporativas vinculantes del controlador para la transferencia de datos personales, WP 264

Comité Europeo de Protección de Datos, CEPD, es un organismo independiente con personalidad jurídica, responsable de garantizar la aplicación coherente del Reglamento general de protección de datos, conforme consta en el artículo 68 y considerando (139) del RGPD.

1. Funcionamiento y organización del Comité

Para el funcionamiento y organización del Comité se han previsto las siguientes consideraciones:

a) Representación y conformación:

a. El Comité estará representado por su Presidente y nombrará a dos vicepresidentes; serán elegidos por mayoría simple de entre sus miembros; tendrá un mandato de cinco años y podrá renovarse una vez. Se ha dicho que, los cinco años también son garantía de independencia pues permiten una continuidad en trabajo ya que en el G29 la presidencia era de apenas 2 años, tiempo insuficiente para cumplir con las funciones a cabalidad. Sin embargo, "la presidencia del Comité no es una función remunerada porque el director de la autoridad nacional elegida para esta función europea sigue ejerciendo sus funciones a nivel nacional, de ahí que el cese a nivel nacional constituya una de las causas de cese en la presidencia del Comité"[766]. Es decir, para el nombramiento del Presidente se deberá revisar el periodo transcurrido de esa autoridad en su país de origen.

b. Estará conformado por:
   a. El Director de una autoridad de control de cada Estado miembro o su representante.
   b. El Supervisor Europeo de Protección de Datos o su representante que será el Secretario del Comité, con lo que se garantiza la independencia del Comité, puesto que conforme Memorando de Entendimiento firmado entre ambas entidades se aclara que el

12. Recomendación sobre el formulario de solicitud estándar para la aprobación de las reglas corporativas vinculantes del procesador para la transferencia de datos personales, WP 265
13. Documento de trabajo que establece una tabla con los elementos y principios que se encuentran en Reglas corporativas vinculantes, WP 256 rev.01
14. Documento de trabajo que establece una tabla con los elementos y principios que se encuentran en las Reglas corporativas vinculantes del procesador, WP 257 rev.01
15. Referencia de adecuación, WP 254 rev.01
16. Directrices sobre la aplicación y fijación de multas administrativas a los efectos del Reglamento 2016/679, WP 253

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, Dictamen 1/2018, 25 de mayo de 2018, accedido el 16/11/2019, https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf

[765] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, Dictamen 1/2018, 25 de mayo de 2018, accedido el 16/11/2019, https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf

[766] L. CERVERA NAVAS, *op.cit*

Supervisor informará y consultará al Comité en materias de relevancia,[767] con lo que se evidencia la primacía del Comité.

c. Si en un Estado miembro existen varias autoridades de control, se nombrará a un representante común de conformidad con el derecho de ese Estado miembro.

b) Participación de la Comisión:

a) La Comisión tendrá derecho a participar en las actividades y reuniones del Comité, sin derecho a voto.
b) La Comisión designará un representante.
c) El presidente del Comité comunicará a la Comisión las actividades del Comité.

Respecto de la toma de decisiones, tal como "se disponía para el Grupo de la Directiva, las decisiones se toman por mayoría simple aunque para algunas decisiones importantes del mecanismo de coherencia o para la propia aprobación del reglamento interno del Comité se exige una mayoría de dos tercios."[768] Resulta evidente que debido a la importancia, deba aprobarse con mayoría calificada, lo relativo al funcionamiento de la propia entidad; sin embargo, supone un reto para la competencia relacionada como la homogeneidad de la aplicación del RGPD, lo que hasta la fecha no ha supuesto un límite para dictar este tipo de resoluciones y se espera que no llegue a serlo.

2. Independencia del Comité

Respecto de la Independencia de Comité, este aspecto fue ampliamente discutido en el momento de elaboración del RGPD, puesto que se consideraba la incorporación del Supervisor como miembro del Comité, podría considerarse como "excesiva y en consecuencia, durante las negociaciones entre el Consejo y el Parlamento Europeo se incluyeron unas salvaguardias para garantizar la independencia operacional del Comité, que no su dependencia administrativa del Supervisor". [769]

Adicionalmente, varias de las funciones del G29 fueron asignadas a dos instituciones, por un lado el CEPD y por otro el Supervisor Europeo de Protección de Datos, como se señala en líneas siguientes:

> […] el Comité Europeo de Protección de Datos supone en la práctica una repartición de funciones entre el sucesor del Grupo y el Supervisor. Mientras el Comité recibe personalidad

[767] *Ibíd.*
[768] L. CERVERA NAVAS, *op.cit.*
[769] *Ibíd.*

jurídica propia y recibe plena independencia del Supervisor Europeo para la toma de decisiones en materia de protección de datos, queda sin embargo apartado de cualquier poder decisión en cuestiones de naturaleza administrativa, que se reservan enteramente para el Supervisor que «se hace cargo de la Secretaría» y decide por tanto sobre la composición y los recursos de la Secretaria, aunque el Memorando de Entendimiento firmado entre ambas entidades aclara que el Supervisor informará y consultará al Comité en materias de relevancia. [770]

Para clarificar la temática el RGPD en su artículo 69 dispone que el Comité actúe con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias, o para la emisión de sus informes (arts. 70 y 71, RGPD).

El Comité no solicitará ni admitirá instrucciones de nadie en el desempeño de sus funciones o el ejercicio de sus competencias.

3. Funciones del Comité

El artículo 70 del RGPD establece como función primordial del Comité garantizar la aplicación coherente del RGPD, para lo cual a iniciativa propia o, en su caso, a instancia de la Comisión realizará las siguientes funciones:

a) Supervisión y garantía
El Comité supervisará y garantizará la correcta aplicación del RGPD en los casos:

a. De resolución de conflictos (art. 64, RGPD).
b. De procedimientos de urgencia (art. 65, RGPD), sin perjuicio de las funciones de las autoridades de control nacionales.

b) Asesoría
El Comité brindará asesoría a la Comisión sobre:

a. Toda cuestión relativa a la protección de datos personales en la Unión.
b. Cualquier propuesta de modificación del Reglamento.
c. El formato y los procedimientos para intercambiar información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes.

[770] *Ibíd.*

c) Directrices, recomendaciones y buenas prácticas

El Comité examinará, de oficio o a instancia de uno de sus miembros o de la Comisión, cualquier cuestión relativa a la aplicación del Reglamento, y emitirá directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del Reglamento sobre:

a. procedimientos para la supresión de vínculos, copias o réplicas de los datos personales procedentes de servicios de comunicación a disposición pública si se cumplen los criterios determinados en el artículo 17, apartado 2 del RGPD, como por ejemplo: ilicitud del tratamiento, no necesarios en relación con los fines, revocatoria del consentimiento, oposición, entre otros;
b. especificar aún más los criterios y requisitos de las decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles que produzcan efectos jurídicos o puedan afectarle significativamente, en virtud del artículo 22, apartado 2 del RGPD;
c. circunstancias probables de que la violación de seguridad de los datos personales constituye un alto riesgo para los derechos y libertades de las personas físicas (art. 34, apdo. 1, RGPD);
d. especificar en mayor medida los criterios y requisitos para las transferencias de datos personales basadas en normas corporativas vinculantes (art. 47, RGPD);
e. especificar en mayor medida los criterios y requisitos de las transferencias de datos personales en ausencia de una decisión de adecuación en una transferencia internacional de datos a un tercer país (art. 49, apdo. 1, RGPD);
f. aplicación de los poderes públicos: de investigación, correctivos, de autorización y colectivos (art. 58, apdos. 1, 2 y 3), y la fijación de multas administrativas, de conformidad con el artículo 83 del RGPD;
g. procedimientos comunes de información procedente de personas físicas sobre infracciones al secreto profesional y confidencialidad de los miembros de las autoridades de control (art. 54, apdo. 2, RGPD).

d) Códigos de conducta, mecanismos de certificación, sellos y marcas de protección.

a. Alentará la elaboración de códigos de conducta y el establecimiento de mecanismos de certificación y de sellos y marcas de protección de datos, de conformidad con los artículos 40 y 42 del RGPD.
b. Emitirá dictámenes sobre los códigos de conducta elaborados y con vigencia en toda la Unión para actos de ejecución en los procedimientos de examen (art. 40, apdo. 9, RGDP).
c. Especificará los requisitos para acreditación de los organismos de certificación, así como realizará la acreditación de los organismos de certificación y su revisión periódica (art. 43, RGPD).
d. Facilitará a la Comisión un dictamen sobre:
    i. los requisitos de certificación contemplados en el artículo 43, apartado 8;

ii. los iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto (art. 12, apdo. 7);
iii. para evaluar la adecuación o no del nivel de protección en un tercer país u organización internacional (art. 70, RGPD).

e) Exámenes y evaluaciones
   a. Constatará las violaciones de la seguridad de los datos y determinar la dilación indebida en el deber de notificar la violación de la seguridad de los datos personales al interesado (art. 33, apdos. 1 y 2, RGPD).
   b. Examinará la aplicación práctica de las directrices, recomendaciones y buenas prácticas sobre la aplicación coherente y para perfiles automatizados de personas físicas.

f) Cooperación y coherencia

   a. Emitirá dictámenes sobre los proyectos de decisión de las autoridades de control, sobre la emisión de dictámenes, la resolución de conflictos y el procedimiento de urgencia, previstos en los artículos, 64, 65 y 66 del RGPD.
   b. Promoverá la cooperación por medio de:
      i. intercambios efectivos de información entre las autoridades de control;
      ii. intercambios efectivos de buenas prácticas entre las autoridades de control;
      iii. programas de formación comunes;
      iv. intercambios de personal entre las autoridades de control y, cuando proceda, con las autoridades de control de terceros países o con organizaciones internacionales;
      v. intercambio de conocimientos;
      vi. intercambio de documentación sobre legislación y prácticas en materia de protección de datos.

   c. Registro, publicación y seguimiento:
      Llevará un registro:

      i. electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia;
      ii. público de los organismos acreditados para otorgar certificación, de los mecanismos de certificación y sellos de protección de datos (art. 43, apdo. 6, RGPD);
      iii. de los responsables o los encargados del tratamiento acreditados o revocados, establecidos en terceros países, en virtud del artículo 42, apartado 7 del RGPD.

d. Transmitirá sus dictámenes, directrices, recomendaciones y buenas prácticas a la Comisión y al Comité y los hará públicos (art. 93, RGPD).
e. Efectuará procedimientos de consulta pública; el Comité consultará a las partes interesadas y les dará la oportunidad de presentar sus comentarios en un plazo razonable y publicará los resultados (art. 76, RGPD).
f. Elaborará un informe anual público en materia de protección de las personas físicas en lo que respecta al tratamiento en la Unión y, si procede, en terceros países y organizaciones internacionales. Y se transmitirá al Parlamento Europeo, al Consejo y a la Comisión (art. 71). El informe anual incluirá un examen de la aplicación práctica de las directrices, recomendaciones y buenas prácticas.

De las atribuciones descritas se puede concluir que el Comité tiene un rol reforzado respecto de su antecesor el G29, por cuanto, lo faculta emitir dictámenes vinculantes para las autoridades nacionales. Pero además, el RGPD si bien otorga un primer filtro a las autoridades de control nacionales, cuando estas no logran resolver sus diferencias, el Comité puede dictar decisiones con el carácter de vinculantes. Lo que permitirá un verdadero trabajo de armonización y aplicación uniforme del RGPD en la Unión Europea. Tal como se señala en el siguiente texto:

> […] en muchas de sus funciones, se asimila a una autoridad (europea) de control por ejemplo cuando emite dictámenes que son vinculantes para las autoridades nacionales, pero, al mismo tiempo, la manera *sui generis* en la que se ha configurado el sistema de gobernanza en el Reglamento hace que, en la inmensa mayoría de los casos, la autoridad competente para decidir en supuestos transnacionales o de ventanilla única, no sea el Comité sino la autoridad principal, pues sólo en aquellos casos (excepcionales) en los que se produzca una discrepancia entre la autoridad principal y las otras autoridades interesadas que no sean capaces de resolver entre ellas mismas, será el Comité el que pasará a resolver la cuestión (véase el mecanismo de resolución de controversias del artículo 65 del Reglamento). [771]

Lo cierto es que el Comité no tiene atribuciones de control *per se,* pues no ejerce de forma directa actividades de vigilancia y sanción sobre responsables de tratamiento ni atiende quejas de titulares de datos, por ejemplo, sino que su finalidad primordial es la de garantizar la aplicación coherente de la legislación.

> […] Se trata de una tarea mucho más específica que la que disponía el artículo 30 de la Directiva, según la cual el Grupo debía «estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea». Así pues, de «contribuir a una aplicación homogénea» se pasa a «garantizar la aplicación coherente» de la legislación. El término «coherente» debe entenderse en el sentido de asegurar una aplicación uniforme por todos los llamados a aplicar el Reglamento, es decir, conforme a la interpretación lógica que se desprende del texto. El significado del término utilizado en la versión inglesa del

[771] *Ibíd.*

> Reglamento «*consistency*» despeja cualquier posible duda al respecto. Para garantizar la aplicación coherente del Reglamento, es decir, la aplicación de la ley de la misma manera, el Comité recibe una larga lista de funciones que se enumeran alfabéticamente de la «a» a la «y». Estas funciones se pueden englobar en tres categorías principales: supervisión, asesoramiento e información […][772]

Para lograr el objetivo de garantizar la aplicación coherente en todos los países miembros de la Unión Europea del RGPD, es indispensable que el Comité asuma el rol que le corresponde, esto es, el de ser coordinador entre las autoridades nacionales de control. Pero además que ejerza con determinación cada una de las funciones previamente descritas, pues solo un Comité activo y dinámico puede afrontar la complejidad no solo de identificar las diferentes interpretaciones y aplicaciones normativas sino de a través de sus resoluciones, recomendaciones y dictámenes brinde soluciones ágiles y eficientes que pueda ser implementadas en todos los países de la Unión.

4. Dictamen del Comité

El artículo 64 del RGPD establece que el Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna de las medidas enumeradas a continuación, para lo cual recibirá el proyecto de decisión que le remita la autoridad de control que tenga por objeto:

a) adoptar una lista de las operaciones de tratamiento que deben realizar una evaluación previa de impacto relativa a la protección de datos de conformidad con el artículo 35, apartado 4;
b) determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el Reglamento (art. 40, apdo. 7);
c) aprobar criterios aplicables a la acreditación de un organismo con arreglo al artículo 41, apartado 3, o un organismo de certificación conforme al artículo 43, apartado 3;
d) determinar las cláusulas tipo de protección de datos contempladas en el artículo 46, apartado 2, literal d), y el artículo 28, apartado 8;
e) autorizar las cláusulas contractuales a que se refiere el artículo 46, apartado 3, literal a);
f) aprobación de normas corporativas vinculantes a tenor del artículo 47;
g) cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro deberá ser examinado por el Comité a efectos de dictamen, en particular cuando una autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua con arreglo al artículo 61 o las operaciones conjuntas con arreglo al artículo 62, y procederá a pedido de cualquier autoridad de control, el presidente del Comité o la Comisión.

[772] *Ibíd.*

En cuanto al procedimiento del dictamen, debe realizarse lo siguiente:

a) Verificar que no se haya emitido ya un dictamen sobre el mismo asunto.
b) Se adoptará por mayoría simple de los miembros del Comité,
c) En el plazo de ocho semanas, que podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto.

5. Resolución de conflictos por el Comité

El artículo 65 del RGPD señala que con el fin de garantizar una aplicación correcta y coherente del Reglamento en casos concretos, el Comité adoptará una decisión vinculante denominada resolución de conflictos, en los siguientes casos:

a) Cuando una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la autoridad principal, o se haya rechazado dicha objeción por no ser pertinente o no estar motivada. La decisión vinculante afectará a todos los asuntos en referencia, en particular si hay infracción del Reglamento.
b) Cuando sea necesario establecer cuál de las autoridades de control interesadas es competente para el establecimiento principal.
c) Cuando una autoridad de control competente no solicite dictamen al Comité sobre los asuntos de su competencia (art. 64, RGPD).
d) Cuando una autoridad de control competente no aplique un dictamen del Comité emitido en los temas de su competencia, en virtud del artículo 64. En tal caso, cualquier autoridad de control interesada, o la Comisión, pondrá en conocimiento de este particular al Comité.

Acerca del procedimiento de resolución de conflictos, debe realizarse lo siguiente:

a) Se tomará la decisión por mayoría de dos tercios de los miembros del Comité.
b) La decisión será vinculante para la autoridad de control principal y a todas las autoridades de control interesadas.
c) La decisión deberá estar motivada.
d) La decisión se adoptará en el plazo de un mes, a partir de la remisión del asunto. Este plazo podrá prorrogarse un mes más, habida cuenta de la complejidad del asunto.
e) Cuando el Comité no haya podido adoptar una decisión en los plazos mencionados, se modificará a mayoría simple y se dará voto dirimente al Presidente.
f) Las autoridades de control interesadas no adoptarán decisión alguna sobre el asunto presentado al Comité.

g) El Presidente del Comité notificará, sin dilación indebida la decisión contemplada, a las autoridades de control interesadas y a la Comisión.
h) La decisión se publicará en el sitio web del Comité sin demora, una vez que la autoridad de control haya notificado la decisión definitiva.
i) La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación adoptará su decisión definitiva, sin dilación indebida y a más tardar un mes tras la notificación de la decisión del Comité.

Tanto los dictámenes como las resoluciones de conflicto como actos normativos vinculantes son herramientas con las que cuenta el Comité para cumplir con su finalidad sustancial de garantizar la aplicación homogénea de RGPD en la Unión Europea. Por ello, se señala que:

> El Comité es mucho más que una «versión 2.0» del Grupo de Trabajo del artículo 29 de la Directiva. Las autoridades nacionales de control pasan de asesorar a la Comisión Europea como un grupo de expertos y bajo la Secretaría de la Comisión a convertirse en los miembros componentes de un organismo de la Unión con la Secretaría del Supervisor Europeo que es también uno de sus miembros. En esta nueva responsabilidad colectiva que tienen las autoridades nacionales de control, el viejo modo de funcionamiento del Grupo, en el que la perspectiva nacional estaba siempre dolorosamente presente, deviene obsoleto y se impone un modo de funcionamiento netamente europeo, transfronterizo, de investigaciones conjuntas y resoluciones directamente aplicables en varios países de la Unión Europea. [773]

Desde esta perspectiva, el Comité debe volcar sus esfuerzos en coordinar con autoridades nacionales, aprovechando su experiencia, especialidad y conocimientos, no solo para la elaboración de dictámenes, resoluciones y recomendaciones, que deben ser aplicados de manera uniforme en la Unión Europea. Sino que, puedan satisfacer las diferentes visiones y necesidades que cada problemática plantea, porque el reto no solo es lograr una uniformidad en la aplicación del RGPD entre países miembros de la Unión, sino sobre todo, en el manejo de una posición única, respecto del flujo transfronterizo de datos. Y es que la visión del Comité ya no puede ser local sino que debe volcarse a los intereses y necesidades comunitarios.

6.10.3 Supervisor Europeo de Protección de Datos

El Reglamento (Ue) 2018/1725 de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, por el que se deroga el Reglamento (CE) n.o 45/2001 y la Decisión n.o 1247/2002/CE crea en su artículo 52, una figura que es ampliamente referenciada en el RGPD, esta es la del Supervisor Europeo de Protección de Datos.

El citado Supervisor tiene la obligación de vigilar todas las operaciones de tratamiento realizadas por instituciones y organismos de la Unión Europea, al tenor de lo que señala el artículo 1 del Reglamento (Ue) 2018/1725 y además velará por que los derechos y libertades fundamentales de las

[773] *Ibíd.*

personas físicas, en particular el derecho de las mismas a la protección de datos, sean respetados por las instituciones y organismos de la Unión, conforme señala el 52 de la norma anterior.

De tal forma que, si el responsable del tratamiento no atiende una solicitud del interesado, comunicará a este más tardar transcurrido un mes a partir de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante el Supervisor Europeo de Protección de Datos y de interponer un recurso judicial, artículo 14 numeral 4.

Asimismo, el responsable de tratamiento asesorará a las instituciones y organismos de la Unión, así como a los interesados, en todas las cuestiones relacionadas con el tratamiento de datos personales (artículo 52) y deberá absolver las consultas de evaluación de impacto, conforme determina el artículo 40 numeral 1.

Conforme el artículo 53 del Reglamento (Ue) 2018/1725 , el Parlamento Europeo y el Consejo nombrarán de común acuerdo al Supervisor Europeo de Protección de Datos por un mandato de cinco años, quien actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus competencias, artículo 54.

Ahora bien, en el marco del RGPD la participación del Supervisor Europeo de Protección de Datos se manifiesta en los siguientes casos:

a) Si el Comité debe dictar una decisión vinculante de conformidad con el artículo 65 del RGPD, el Supervisor Europeo de Protección de Datos solo tendrá derecho a voto en las decisiones relativas a los principios y normas aplicables a las instituciones, órganos y organismos de la Unión. El haber establecido limitaciones en su participación en el Comité permite establecer la independencia del Comité.

   Justamente como mecanismo de cautela para impedir injerencias del Supervisor se estableció:

   > […] la necesidad de que existiera un superior jerárquico distinto sobre el personal del Supervisor que desempeñase las funciones conferidas al Comité (párrafo tercero del artículo 75), y se dijo explícitamente que la Secretaría «ejercerá sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité» (párrafo segundo), haciendo por tanto imposible la injerencia por parte de los Supervisores sobre el personal afecto al funcionamiento del Comité. [774]

[774] *Ibíd.*

b) Estará a cargo de la Secretaría del Comité (considerando [140], RGDP).

c) Para clarificar la relación entre Comité y Supervisor se firmó un memorando de entendimiento que establece entre otras especificaciones aquella que determina que, el "Comité es soberano en cuestiones operacionales mientras que la responsabilidad administrativa"[775] es del Supervisor, quien, por ejemplo, tiene la responsabilidad de dotar el personal y los medios financieros necesarios para el funcionamiento del Comité. En este sentido, se ha señalado que:

> Es importante destacar que la expresión «hacerse cargo de la secretaría del Comité» utilizada en el Reglamento constituye una responsabilidad activa por parte del Supervisor que va más allá de «poner a disposición» del Comité unos medios humanos y materiales y que va más allá de las tareas que se encargan a la secretaría en el párrafo sexto del artículo 75. Existen tareas logísticas y administrativas muy importantes tales como la preparación, defensa e implementación del presupuesto del Comité; procedimientos de recursos humanos tales como la selección y la contratación, u otras funciones administrativas propias de las instituciones y organismos de la UE que no aparecen recogidas en el texto del Reglamento y que, sin embargo, son responsabilidad del Supervisor y así vienen específicamente recogidas en el memorando de entendimiento. [776]

De lo analizado, la figura del Supervisor Europeo de Protección de Datos, aunque no es nueva y ha sido reconocida en una norma distinta al RGPD, es parte de la institucionalidad de protección, es decir de las autoridades de control, vigilancia, protección y desarrollo, no solo la vigencia jurídica sino la defensa de los derechos de los titulares de los datos personales.

6.10.4 Comisión Europea

La Comisión Europea (en adelante, la Comisión), reconocida en el Tratado de Funcionamiento de la Unión Europea,[777] es un órgano ejecutivo y políticamente independiente:

> [...] encargado de defender el interés general de la Comunidad en el seno de la estructura institucional, [...] difiere de las secretarías generales de las organizaciones internacionales y es equiparable a los gobiernos o ejecutivos de los sistemas constitucionales internos. Su organización y funcionamiento, así como las competencias que le ha sido atribuida, le

[775] *Ibíd.*
[776] *Ibíd.*
[777] TRATADO DE LA UNIÓN EUROPEA, T*ratado de la Unión Europea OJ C 191*, 29 de julio de 1992, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:11992M/TXT.

confieren un papel central en el proceso de integración comunicación, que le ha hecho merecedora del calificación de «motor de la Comunidad».[778]

Entre las prioridades establecidas por la Comisión Europea consta la atinente a Justicia y Derechos fundamentales, en la cual el derecho a la protección de datos es uno de los temas que ha cobrado mayor relevancia a partir de la promulgación del RGPD; incluso se creó un nuevo organismo analizado previamente: el Comité Europeo de Protección de Datos.

Entre las funciones de la Comisión —las aplicables al presente trabajo de investigación— se encuentran: promover propuestas de nueva legislación para proteger los intereses de la Unión Europea y a sus ciudadanos; aplicar y verificar la implementación de la normativa europea y de las decisiones del Parlamento Europeo y del Consejo de Europa.

1. Funciones de la Comisión en materia de protección de datos establecidas por el RGPD

La Comisión Europea tiene competencias para pronunciarse sobre temas que tienen efectos en toda la Unión Europea. El RGPD establece a lo largo de la normativa que regula la institucionalidad de protección varias funciones que la Comisión asume a partir de su vigencia, las cuales son:

a) Decidir sobre si un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional ofrece o no un nivel de protección de datos adecuado; decisión que puede ser revocada y que permite para realizar transferencias de datos personales con estos países sin necesidad de otro tipo de autorización (considerandos [103], [168] y art. 70, lit. s), RGPD).
b) El considerando (104) del RGPD señala que el tercer país debe ofrecer un nivel adecuado de protección equivalente, en lo esencial, a lo ofrecido en la Unión. Es decir, independencia de la autoridad de control, mecanismos de cooperación con autoridades de control, derechos, acciones administrativas y judiciales efectivas, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos.
c) Solicitar al Comité la emisión de un Dictamen en cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro, al tenor del artículo 64, numeral 2 del RGPD.
d) Solicitar al Comité la emisión de un Dictamen cuando una autoridad de control competente incumpla las obligaciones relativas a asistencia mutua (art. 61, operaciones conjuntas, art. 62, RGPD).
e) Derecho a participar en las actividades y reuniones del Comité Europeo de Protección de Datos, sin derecho a voto, por intermedio del representante que designará para el efecto (art. 68, num. 5, RGPD).

[778] M. DE VELASCO, *Las organizaciones internacionales* (Madrid: Tecnos, 2007).

f) Solicitar, en un plazo determinado por la Comisión, la asesoría del Comité sobre toda cuestión relativa a la protección de datos personales en la Unión, en particular sobre cualquier propuesta de modificación al Reglamento (art. 70, num. 1, lit. b), RGPD).

g) Solicitar al Comité un dictamen sobre los requisitos de certificación contemplados en el artículo 43, apartado 8, artículo 70, literal q) del RGPD.

h) Solicitar al Comité un dictamen sobre los iconos a que se refiere el artículo 12, apartado 7, artículo 70, literal r) del RGPD.

i) Mediante actos de ejecución (considerando [168], RGPD), que son mecanismos que permiten establecer condiciones uniformes de aplicación de una ley en la Unión Europea[779] y que se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2), conforme el artículo 61, numeral 9, la Comisión podrá:

   a. especificar el formato;
   b. los procedimientos de asistencia mutua;
   c. las modalidades del intercambio de información por medios electrónicos entre las autoridades de control y entre las autoridades de control y el Comité (art. 67, RGPD);
   d. el formato normalizado de intercambio de información entre autoridades de control (art. 67, RGPD).

j) Mediante actos delegados, que es un "tipo de disposición que la Comisión adopta en virtud de una delegación otorgada a través de una ley de la Unión Europea",[780] que podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo y que en el presente caso ha sido entregada por tiempo indefinido a partir del 24 de mayo de 2016, conforme artículo 92 del RGPD, la Comisión estará facultada a:

   a. especificar la información que se ha de presentar mediante iconos y los procedimientos para proporcionar iconos normalizados (art. 12, apdo. 8, RGPD);
   b. especificar las condiciones que deberán tenerse en cuenta para los mecanismos de certificación en materia de protección de datos (art. 42, apdo. 1, RGPD).

k) Presentar un informe público al Parlamento Europeo y al Consejo, a más tardar el 25 de mayo de 2020 y posteriormente cada cuatro años, sobre la evaluación y revisión del Reglamento (art. 97, RGPD).

l) Realizar evaluaciones y revisiones sobre la aplicación y el funcionamiento de las mismas, que serán parte del informe:

[779] COMISIÓN EUROPEA, *Actos de ejecución y actos delegados*, accedido 12 de octubre de 2018, https://ec.europa.eu/info/law/law-making-process/adopting-eu-law/implementing-and-delegated-acts_es.
[780] Actos de ejecución y actos delegados.

a. la transferencia de datos personales a países terceros u organizaciones internacionales (art. 45, apdo. 3, RGPD);
b. los mecanismos de cooperación y coherencia.

m) Solicitar información a los Estados miembros y a las autoridades de control con miras a realizar la evaluación y revisión de RGPD y emitir el informe correspondiente (art. 97, RGPD).
n) Presentar las propuestas de modificación del Reglamento, de ser necesario, teniendo en cuenta la evolución de las tecnologías de la información y los progresos en la sociedad de la información (art. 97).
o) Presentar propuestas legislativas, de ser el caso, para modificar otros actos jurídicos de la Unión sobre protección de datos, tratamiento por parte de las instituciones, órganos y organismos de la Unión, y respecto de la libre circulación de datos, a fin de velar por una normativa uniforme y coherente (art. 98).

2. Comunicaciones, notificaciones e informaciones que deben ser puestas en conocimiento de la Comisión

La Comisión deberá ser informada mediante comunicaciones, notificaciones e informaciones sobre los siguientes asuntos que deben elevarse a su conocimiento:

a) La Presidencia del Comité, sin dilación indebida, informará y hará público por medios electrónicos cada dictamen, directriz, recomendación y buenas prácticas que emita, tanto a la autoridad de control como a la Comisión (art. 64, num. 5 y art. 70, num. 3, RGPD).
b) Una autoridad de control interesada, sin dilación, comunicará junto con los motivos de su adopción, las medidas provisionales, tomadas dentro de un proceso urgente y que tengan por finalidad producir efectos jurídicos en su propio territorio, en un período de validez determinado no superior a tres meses, a las demás autoridades de control interesadas, al Comité y a la Comisión (art. 66, RGPD).
c) Cada Estado miembro notificará a la Comisión las disposiciones legislativas que se adopten hasta antes del 25 de mayo de 2018; y a partir de esta fecha, sin dilación y en adelante, cualquier modificación posterior, legislativa u otra, de las mismas relativas a:

a. sanciones aplicables a las infracciones del Reglamento (art. 84, num. 2, RGPD);
b. para la conciliación por ley del derecho a la protección de los datos personales y el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria (art. 85, num. 3, RGPD);
c. el tratamiento de datos personales de los trabajadores en el ámbito laboral (art. 88, num. 3, RGPD);

d. obligación de secreto profesional o a otras obligaciones de secreto equivalentes (art. 90, RGPD).

3. Mecanismos de coherencia

Mediante una aplicación coherente del RGPD, las autoridades de control cooperarán entre sí y con la Comisión (art. 51). De modo que implementarán los mecanismos de coherencia establecidos en el artículo 63.

El considerando (123) determina que la finalidad de los mecanismos de coherencia es otorgar un marco uniforme de protección para las personas en el tratamiento de sus datos personales, y al mismo tiempo facilitar la libre circulación de los datos personales en el mercado interior. Vale la pena anotar que para la implementación de estos mecanismos de coherencia o de asistencia mutua, no hace falta acuerdo alguno entre los Estados miembros.

6.11 Régimen sancionador

El RGPD establece un régimen con sanciones económicas altas. Sobre si la propuesta normativa está lejos aún de determinar su efectividad, solo el paso del tiempo podrá dar la razón a quienes sostienen que las multas son excesivas y que afectan, sobre todo, a las pequeñas y medianas empresas e incluso al consumidor o que, por el contrario, son mecanismos que unidos a otros presentes en el reglamento intentan en su conjunto hacer universal esta normativa, como aquellos artículos relativos al ámbito de aplicación, la seguridad y los datos transfronterizos. Mucho se ha hablado de las multas altas[781] que impone la normativa, sobre su efectividad a la hora de intentar frenar actuaciones indebidas de quienes ostentan la mayor acumulación de datos en el mundo, refiriéndose a plataformas como Facebook y Google;[782] sin embargo, es innegable que la mayor innovación de esta normativa es el reforzamiento del régimen sancionador (considerando [11], RGPD), puesto que:

> [...] la protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes.

[781] "La resaca del nuevo Reglamento de Protección de Datos: «Esto es un caos»", *El Mundo*, 29 de mayo de 2018, http://www.elmundo.es/tecnologia/2018/05/29/5b0bd534268e3e40068b4580.html.
[782] "El usuario, la verdadera víctima del RGPD", *Marketing Directo* (blog), 25 de mayo de 2018, https://www.marketingdirecto.com/digital-general/digital/el-usuario-la-verdadera-victima-del-rgpd.

Por su parte, el artículo 83 RGPD sobre la normativa propone que cada autoridad de control garantice que la imposición de las multas administrativas sea individual y efectiva, así como que resulten proporcionadas y disuasorias.

En ese sentido, el mayor reto que enfrenta el RGPD es convencer —a título de concienciación o mediante la coacción sancionatoria— que la cultura de la protección de datos debe convertirse en un actuar obvio por parte de responsables y encargados, y que de nada sirve tener datos de las personas sino se tiene su confianza. Desde esta perspectiva, las multas no son altas sino mecanismos disuasorios eficientes, puesto que en tecnología todo se basa en costos de implementación, de tal manera que, resulte económicamente más rentable realizar procesos de adaptación y de modificación de la conducta a un enfoque proactivo de protección, que pagar multas, no solo por el costo económico que esto significa, sino por el valor más importante que un responsable o encargado de tratamiento tiene: su reputación y su credibilidad.

6.11.1 Sanciones administrativas mediante poderes correctivos

Aunque ya se analizó anteriormente la cuestión de los poderes públicos que ostenta una autoridad de control, por ser parte del régimen sancionatorio, es indispensable volver con este análisis. En el artículo 58, numeral 2 del RGPD, se establece que cada autoridad de control dispondrá a responsables y encargados del tratamiento una o varias de las sanciones simultáneas, mediante los siguientes poderes correctivos indicados a continuación y que he clasificado según el tipo de transgresión que las genera:

a) Sobre operaciones de tratamiento

   a. Emitir una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el RGPD.
   b. Emitir un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el RGPD. El considerando (148) del RGPD establece que "en caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento".
   c. Ordenar que las operaciones de tratamiento se ajusten a las disposiciones del RGPD en la forma y en un plazo especificado.
   d. Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.

b) Sobre derechos del interesado
   a. Ordenar que atiendan las solicitudes de ejercicio de los derechos del interesado.
   b. Ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales.

c. Ordenar la rectificación o supresión de datos personales o la limitación de tratamiento y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales.

c) Sobre certificaciones
    a. Retirar directamente, de ser el caso, una certificación si no se cumplen o dejan de cumplirse los requisitos.
    b. Ordenar al organismo de certificación que retire una certificación, si no se cumplen o dejan de cumplirse los requisitos.
    c. Ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos.

d) Datos transfronterizos
    a. Ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

6.11.2 Condiciones generales para la imposición de multas administrativas

Al tenor de lo señalado en el artículo 83 del RGPD, para la imposición de multas administrativas y su cuantía la autoridad de control deberá:

a) Sobre cuestiones generales
    a. Atender las circunstancias de cada caso individual.
    b. Definir si las multas se impondrán de forma adicional o sustitutiva de aquellas medidas contempladas en el artículo 58, apartado 2, literales a), h) y j), RGPD, revisados en el acápite anterior.
    c. Aplicar otras sanciones, conforme cada Estado miembro determine en su normativa interna, en especial si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.
b) Sobre las características de la infracción
    a. La naturaleza, gravedad y duración de la infracción.
    b. La naturaleza, alcance o propósito de la operación de tratamiento de que se trate.
    c. Las categorías de los datos de carácter personal afectados por la infracción.
    d. El número de interesados afectados.
    e. El nivel de los daños y perjuicios que hayan sufrido los interesados afectados.
    f. La intencionalidad o negligencia en la infracción.

c) Sobre las responsabilidades de la infracción
    a. El grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado los principios de privacidad por defecto y por diseño y de seguridad, artículos 25 y 32, respectivamente.

b. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

d) Sobre factores agravantes
   a. Toda infracción anterior cometida por el responsable o el encargado del tratamiento, a modo de reincidencia.
   b. Cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas.
   c. Cualquier otro factor agravante aplicable a las circunstancias del caso, como los perjuicios financieros o las directas o indirectas, mediante la infracción.

e) Sobre factores atenuantes
   a. Cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados.
   b. El grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción.
   c. La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida.
   d. La adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42.
   e. Cualquier otro factor atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, mediante la infracción.

f) Sobre coherencia
   a. El considerando (150) del RGPD señala que una forma de reforzamiento y armonización es autorizar que cada autoridad de control debe estar facultada para imponer multas administrativas.
   b. Las autoridades de control deberán activar el mecanismo de coherencia para fomentar una aplicación coherente de las multas administrativas.
   c. Cada Estado miembro debe determinar si y en qué medida se debe imponer multas administrativas a las autoridades públicas, aclarándose que de forma expresa consta la salvedad de que una autoridad pública reciba una multa administrativa o una advertencia no afecta al ejercicio de otras competencias ni a la aplicación de otras sanciones (considerando [150] y art. 83, num. 2, RGPD).

En general, la imposición de sanciones administrativas y de multas se sujetará a las garantías procesales, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías, considerando (48) del RGPD.

6.11.3 Infracciones y multas administrativas

El artículo 83 del RGPD establece que las autoridades de control pueden imponer, además de las sanciones administrativas de forma simultánea o independiente, multas administrativas, a excepción de Dinamarca y Estonia, en donde estas deberán ser impuestas por tribunales nacionales competentes en cuanto sanción penal. En Estonia la multa será impuesta por la autoridad de control en el marco de un juicio de faltas, de conformidad con el considerando (151) del RGPD.

La citada norma señala dos categorías de multas administrativas, de modo que la legislatura efectuó un análisis de ponderación para determinar qué infracciones ameritan una cuantía más elevada de multa respecto de otras. Entonces, se establecen las siguientes condiciones aplicables de manera general:

a) Un monto máximo de multa que oscila entre 10 000 000 EUR a 20 000 000 EUR para personas naturales o para empresas.
b) Una cuantía equivalente del 2% al 4% del volumen de negocio total anual global del ejercicio financiero anterior, como máximo; solo para empresas.
c) En caso de diferencia entre el monto en euros o la cuantía equivalente en porcentaje del volumen de negocio total anual global del ejercicio financiero anterior, se optará por la cuantía mayor.

Con la finalidad de identificar las infracciones, las sanciones y verificar su proporcionalidad, consta a continuación un cuadro en el que se encuentra categorizada esta información por responsable, encargado, organismos de certificación y autoridad de control.

Normativa	Temática	Infracciones a:	Norma	Infractor	Monto máximo de multa	Porcentaje de multa si se trata de una empresa	
Art. 83, num. 4, lit. a), RGPD.	Tratamiento	Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.	Artículo 8, RGPD.	Obligaciones del responsable y del encargado.	10 000 000 EUR como máximo.	Cuantía equivalente al 2 %	Como máximo del volumen de negocio total anual global del ejercicio financiero anterior.
		Tratamiento que no requiere identificación.	Artículo 11, RGPD.				
		Protección de datos desde el diseño y por defecto.	Artículo 25, RGPD.				
	Delegado de Protección de Datos	Funciones del delegado de protección de datos.	Artículo 39, RGPD.				
	Certificaciones	Certificación.	Artículo 42, RGPD.				
		Organismos de certificación.	Artículo 43, RGPD.				
Art. 83, num. 4, lit. b), RGPD.	Certificaciones	Certificación.	Artículo 42, RGPD.	Obligaciones de los organismos de certificación.			
		Organismos de certificación.	Artículo 43, RGPD.				
Art. 83, num. 4, lit. b), RGPD.	Código de conducta	Supervisión de código de conductas aprobado.	Artículo 41, apartado 4 RGPD.	Obligaciones de la autoridad de control.			
Art. 83, num. 5, lit. a), RGPD.	Principios del tratamiento	Definiciones.	Artículo 4, RGPD.	Obligaciones del responsable y del encargado.	20 000 000 EUR como máximo.	Cuantía equivalente al 4 %	Como máximo del volumen de negocio total anual global del ejercicio financiero anterior.
		Principios relativos al tratamiento.	Artículo 5, RGPD.				
		Licitud del tratamiento.	Artículo 6, RGPD.				
		Condiciones para el consentimiento.	Artículo 7, RGPD.				
		Tratamiento de categorías especiales de datos personales.	Artículo 9, RGPD.				
Art. 83, num. 5, lit. b), RGPD.	Derechos de los interesados	Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.	Artículo 12, RGPD.				
		Información que deberá facilitarse cuando los datos personales se obtengan del interesado.	Artículo 13, RGPD.				
		Información que deberá facilitarse cuando los datos personales no se	Artículo 14, RGPD.				

		hayan obtenido del interesado.					
		Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.	Artículo 15, RGPD.				
		Derecho de rectificación.	Artículo 16, RGPD.				
		Derecho de supresión («el derecho al olvido»).	Artículo 17, RGPD.				
		Derecho a la limitación del tratamiento.	Artículo 18, RGPD.				
		Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.	Artículo 19, RGPD.				
		Derecho a la portabilidad de los datos.	Artículo 20, RGPD.				
		Derecho de oposición.	Artículo 21, RGPD.				
		Decisiones individuales automatizadas, incluida la elaboración de perfiles.	Artículo 22, RGPD.				
Art. 83, num. 5, lit. c), RGPD.	Transferencias de datos personales a un destinatario en un tercer país o una organización internacional.	Principio general de las transferencias.	Artículo 44, RGPD.				
		Transferencias basadas en una decisión de adecuación.	Artículo 45, RGPD.				
		Transferencias mediante garantías adecuadas.	Artículo 46, RGPD.				
		Normas corporativas vinculantes.	Artículo 47, RGPD.				
		Transferencias o comunicaciones no autorizadas por el Derecho de la Unión.	Artículo 48, RGPD.				
		Excepciones para situaciones específicas.	Artículo 49, RGPD.				
Art. 83, num. 5, lit. d), RGPD.	Toda obligación en virtud del derecho de los Estados miembros que se adopte con arreglo al capítulo IX: Disposiciones relativas a situaciones específicas de	Tratamiento y libertad de expresión y de información.	Artículo 85, RGPD.				
		Tratamiento y acceso del público a documentos oficiales.	Artículo 86, RGPD.				
		Tratamiento del número nacional de identificación.	Artículo 87, RGPD.				
		Tratamiento en el ámbito laboral.	Artículo 88, RGPD.				
		Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.	Artículo 89, RGPD.				

	tratamiento.	Obligaciones de secreto.	Artículo 90, RGPD.				
		Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas.	Artículo 91, RGPD.				
Art. 83, num. 5, lit. e), RGPD.	Poderes correctivos.	Incumplimiento de una resolución control.	Artículo 58, apartado 2, RGPD.				
		Incumplimiento de una limitación temporal o definitiva del tratamiento.					
		Incumplimiento de la suspensión de los flujos de datos por parte de la autoridad de control.					
	Poderes de investigación.	No facilitar acceso para acciones de investigación.	Artículo 58, apartado 1, RGPD.				
Art. 83, num. 6, RGPD.	Resoluciones sobre sanciones dictadas con poderes correctivos.	Incumplimiento de las resoluciones de la autoridad de control.	Artículo 58, apartado 2, RGPD.				

Del cuadro precedente se concluye que en la ponderación realizada por el legislador para determinar el tipo de infracción en su relación con la cuantía de multa establecida, los criterios a los que se atribuye mayor gravosidad son aquellos relacionados con: los principios del tratamiento, los derechos de los interesados, la transferencia internacional de datos personales, situaciones específicas de tratamiento como la libertad de expresión, o los datos laborales, entre otros. Es decir, aquellos elementos cuya violación representan un grave riesgo o daño para la persona titular del dato.

Pero, asimismo, se aplica mayor nivel de multa en los casos de incumplimiento de poderes correctivos y de investigación, y en general el incumplimiento de las resoluciones sobre sanciones dictadas con poderes correctivos, como una forma de empoderar a los órganos de control para que las instituciones acaten las disposiciones que se emitan y puedan cumplir con su finalidad.

De otro lado, una de las mejoras que los especialistas han visibilizado respecto de las administraciones públicas consiste en:

> […] el RGPD viene a acabar, al menos en lo que a la redacción de sus preceptos se refiere, con el diferente régimen sancionador establecido por la normativa actual, para las infracciones cometidas por las entidades de derecho privado y por las de derecho público. En este sentido, el artículo 83.7 del RGPD, establece la capacidad de las autoridades de control de imponer multas administrativas, esto es, sanciones económicas (como en el caso de las empresas privadas), a autoridades y organismos públicos establecidos en los Estados miembros, que así lo hayan establecido. Es decir, el RGPD otorga a los Estados miembros la capacidad de establecer normas respecto a si se puede imponer multas administrativas a la administración pública (lógicamente de dicho Estado) y, en su caso, la medida de las mismas.[783]

Sin duda, el sector público es uno de los grandes responsables de bases de datos y en esta perspectiva es necesario que existen mecanismos eficaces que disuadan un actuar enmarcado en el cumplimiento de la norma. Por ello, si bien el RGPD establece la facultad de cada Estado de incorporar en sus legislaciones la posibilidad de imponer multas administrativas, y en este supuesto pareciera imposible de ejecutar porque estos recursos serían gravosos y en la práctica volverían al erario público, por lo que se avizora el paulatino establecimiento de condiciones de otras medidas ejemplificadoras equivalentes.

Finalmente, el artículo 84 del RGPD estipula que cada Estado miembro podrá establecer normas que contengan otras sanciones aplicables, en especial para aquellas infracciones en la que no se sancionen con multas administrativas de conformidad con el artículo 83, y que mediante ella se pueda lograr su cumplimiento. Además, al tenor de lo señalado en los considerandos (149) y (152) del RGPD, los Estados miembros deben tener la posibilidad de establecer infracciones y

[783] S.VASQUEZ Y J. MIGUEL, *Nuevo Régimen Sancionador de Protección de Datos*, (España: Economist & Jurist, 2019 , 26.

sanciones de carácter penal relacionadas con el Reglamento, siempre y cuando eviten la vulneración del principio *non bis in ídem*.

6.12 Delegado de protección de datos personales

Sobre el delegado de protección de datos personales, en adelante DPD, se analizará a continuación las condiciones para su designación, nombramiento, funciones y características propias definidas en el RGPD y que han sido ampliadas y explicadas por parte del Grupo de trabajo sobre protección de datos del artículo 29, G29; a través de las Directrices sobre oficiales de protección de datos, emitidas el 13 de diciembre de 2016, y revisadas y adoptadas el 5 de abril de 2017, las cuales, incluso han sido avaladas por el CEPD.

En dichas directrices consta que "el concepto de DPD no es nuevo. Aunque la Directiva 95/46/CE3 no exigía a ninguna organización el nombramiento de un DPD, la práctica de tal designación se ha desarrollado, no obstante, en varios Estados miembros a lo largo de los años".[784]

La primer vez que se menciona el concepto de DPD es en el Documento de Trabajo sobre evaluación de impacto del Reglamento del Parlamento Europeo y del Consejo sobre la protección de individuos con respecto al procesamiento de datos personales y a la libre circulación de dichos datos y la Directiva del Parlamento Europeo y del Consejo sobre la protección de las personas con respecto al procesamiento de datos personales por parte de las autoridades competentes para los fines de prevención, investigación, detección o enjuiciamiento de delitos penales o la ejecución de sanciones penales y la libre circulación de dichos datos, en el cual al definir al Oficial de protección de datos, DPO se lo conceptualiza como:

> […] una persona responsable dentro de un controlador de datos o un dato procesador para supervisar y monitorear de manera independiente la aplicación interna y el respeto de las normas de protección de datos. El DPO puede ser un empleado interno o externo consultor.[785]

[784] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Directrices sobre oficiales de protección de datos ('DPO')*, WP243 rev.01, 5 de abril de 2017, accedido el 16 de noviembre de 2019 en https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

[785] COMISIÓN EUROPEA, *Documento de Trabajo sobre evaluación de impacto del Reglamento del Parlamento Europeo y del Consejo sobre la protección de individuos con respecto al procesamiento de datos personales y a la libre circulación de dichos datos y la Directiva del Parlamento Europeo y del Consejo sobre la protección de las personas con respecto al procesamiento de datos personales por parte de las autoridades competentes para los fines de prevención, investigación, detección o enjuiciamiento de delitos penales o la ejecución de sanciones penales y la libre circulación de dichos datos,* Bruselas, 25 de enero de 2012, accedido el 16 de noviembre de 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN

Por su parte, "tanto la conocida LORTAD como la LOPD optaron por la fórmula del Registro Público de ficheros o tratamientos en lugar de la alternativa de contar con los delegados de protección de datos. Y, sin embargo, eso no significó que desde un punto de vista práctica la figura no existiese en nuestro país"[786]. Esta afirmación, sustenta que siendo España líder en protección de datos personales, a través de la implementación de las normativas de protección, logró formar profesionales especializados.

La figura del DPD es parte del sistema de rendición de cuentas por el cual los responsables del tratamiento establecen mecanismos que permitan demostrar su voluntad de prevenir transgresiones a los derechos de los titulares de los datos personales. De esta manera, "la clave es la «proactividad»: han de poder demostrar el cumplimiento de todos sus deberes u obligaciones (accountability), y han de implementar todo tipo de medidas para garantizar el correcto ejercicio de sus obligaciones,"[787] entre las que, los DPD tiene un sitial destacado, pues no solo sirve de medio demostrativo sino que es un mecanismo con el cual se puede, de forma oportuna, evitar situaciones dañosas.

Entonces, el DPD nació como un mecanismo o buena práctica de quienes creían en la transparencia como unos de sus principios institucionales. Era una figura probada, pues en varios países ya era obligatoria su implementación y en otros opcionales[788], pero lo cierto es que varias entidades ya la usaban y por ello el G29, antes incluso de la adopción del RGPD, señaló que:

> […] es la piedra angular de la rendición de cuentas y que el nombramiento de un DPD puede facilitar el cumplimiento y, además, convertirse en una ventaja competitiva para las empresas. Además de facilitar el cumplimiento mediante la aplicación de instrumentos de rendición de cuentas (tales como facilitar o llevar a cabo evaluaciones de impacto y auditorías de protección de datos), los DPD actúan como intermediarios entre las partes interesadas correspondientes (p. ej. autoridades de control, interesados y unidades de negocio dentro de una organización). [789]

El DPD responde a las nuevas formas de organización mundial y representa una oportunidad de emprender en nuevas formas laborales o empresariales, ya que la:

---

[786] R. MARTÍNEZ, "El delegado de protección de datos", *Tratado de protección de datos,* Coordinador: A. RALLO LOMBARTE, (Valencia: Tirant lo Blanch on line, 2019)

[787] J. APARICIO VAQUERO, "La protección de datos que viene: el nuevo Reglamento General europeo", *Ars Iuris Salmanticensis*, volumen 4, (diciembre 2016), 32

[788] "En España nuestra normativa de protección de datos no contempló esta posibilidad como sí lo hicieron, por ejemplo, la Húngara y la Alemana puesto que la regulación europea, la derogada Directiva 95/46/CE19, no exigía su establecimiento a ninguna organización, por lo que en otros países como Holanda o Austria su nombramiento era opcional, y en otros como España no se exigía con anterioridad a la entrada en vigor del nuevo Reglamento UE 2016/679 de 25 de mayo de 2018".

E. SIERRA BENÍTEZ, "El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico", *Revista internacional y comparada de relaciones laborales y derecho del empleo,* Volumen 6, núm. 1, (enero-marzo de 2018): 243

[789] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *op. cit.*.

> […] denominada revolución telemática comporta no sólo la desaparición de antiguos oficios sino la creación de nuevos trabajos y oportunidades, e incluso a la creación de nuevas empresas especializadas en el área de la salvaguarda de la protección de datos. Dada la importancia que va cobrando con el paso del tiempo la materia de protección de datos nos encontramos ante una nueva rama profesional con un brillante futuro.[790]

Es decir, el delegado de protección de datos es una figura positiva porque ha demostrado no solo su eficacia como mecanismo de transparencia sino porque resulta útil y dinámica para resolver las situaciones que, en el día a día, se presentan sobre el uso adecuado de los datos personales y por ende resulta un mecanismo idóneo de garantía y control de los derechos de las personas y además apuntala un nuevo nicho laboral y empresarial en la sociedad del conocimiento.

6.12.1 Condiciones para la designación del delegado de protección de datos personales:

El artículo 37 del RGPD determina la obligación del responsable y el encargado del tratamiento de designar al citado delegado cuando se cumpla una de las siguientes circunstancias:

1. *El tratamiento lo realice una autoridad pública o un organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.*

   Al respecto, el G29 señala que debido a que el RGPD "no define qué constituye una «autoridad u organismo público». El Grupo de Trabajo del artículo 29 considera que dicha noción debe determinarse en virtud del Derecho nacional". [791] En tal sentido, de manera general, las normativas locales señalan que, cumplen funciones públicas aquellos entes privados que actúan por delegación, como: los servicios de agua potable y luz eléctrica, por ejemplo, y tal como señala el propio G29 resulta evidente que "las personas suelen tener un poder de decisión igualmente escaso o nulo sobre si sus datos se tratan y de qué manera, y pueden, por tanto, requerir la protección adicional que pueda aportar la designación de un DPD" [792] Por ello, se recomienda "como buena práctica que las organizaciones privadas que llevan a cabo una función pública o ejercen autoridad pública designen un DPD". [793]

   De otro lado, el G29 determina que el DPD asignado a instituciones públicas tiene competencia sobre los tratamientos de la institución en general, independientemente "de que estos no estén relacionados con el desempeño de una función pública o el ejercicio de una autoridad pública (p. ej. la gestión de una base de datos de empleados)". [794]

[790] F. GUDÍN RODRÍGUEZ-MAGARIÑO, *op. cit.*
[791] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *op.cit*, accedido el 16 de noviembre de 2019 en https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
[792] *Ibíd.*
[793] *Ibíd.*
[794] *Ibíd.*

2. *Las actividades principales consistan en el tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.*

Es decir, es obligatorio designar un DPD si se trata de actividades principales y no cuando estas sean secundarias. Ahora bien, el G29 aclara que debe entenderse por actividades principales señalando que son aquellas operaciones:

> […] clave necesarias para lograr los objetivos del responsable o del encargado del tratamiento. No obstante, las «actividades principales» no deben interpretarse como excluyentes cuando el tratamiento de datos sea una parte indisociable de la actividad del responsable o encargado del tratamiento. Por ejemplo, la actividad principal de un hospital es prestar atención sanitaria. Sin embargo, un hospital no podría prestar atención sanitaria de manera segura y eficaz sin tratar datos relativos a la salud, como las historias clínicas de los pacientes. Por tanto, el tratamiento de dichos datos debe considerarse una de las actividades principales de cualquier hospital y los hospitales deben, en consecuencia, designar un DPD. [795]

De lo dicho, se colige que, aquellas actividades secundarias que no ameritan la designación obligatoria de un DPD se refieren a las de orden administrativo o de apoyo que permiten el desarrollo habitual de la actividad principal, como el pago de remuneraciones de empleados[796] o la asignación de bienes de uso laboral.

De otro lado, esta condición de designación obligatoria de un responsable de tratamiento también utiliza la frase "observación habitual y sistemática". Por lo que, nuevamente ante la falta de definición de esta terminología:

> El Grupo de Trabajo del artículo 29 interpreta «habitual» con uno o más de los siguientes significados: continuado o que se produce a intervalos concretos durante un periodo concreto; recurrente o repetido en momentos prefijados; que tiene lugar de manera constante o periódica. El Grupo de Trabajo interpreta «sistemático» con uno o más de los siguientes significados: que se produce de acuerdo con un sistema; preestablecido, organizado o metódico; que tiene lugar como parte de un plan general de recogida de datos; llevado a cabo como parte de una estrategia.[797]

Como ejemplos de estas actividades el G29 señala los siguientes:

[795] *Ibíd.*
[796] *Ibíd.*
[797] *Ibíd.*

> […] operar una red de telecomunicaciones; prestar servicios de telecomunicaciones; redireccionar correos electrónicos; actividades de mercadotecnia basadas en datos; elaborar de perfiles y otorgar puntuación con fines de evaluación de riesgos (p. ej. para determinar la calificación crediticia, establecer primas de seguros, prevenir el fraude, detectar blanqueo de dinero); llevar a cabo un seguimiento de la ubicación, por ejemplo, mediante aplicaciones móviles; programas de fidelidad; publicidad comportamental; seguimiento de los datos de bienestar, estado físico y salud mediante dispositivos ponibles; televisión de circuito cerrado; dispositivos conectados, como contadores inteligentes, coches inteligentes, domótica, etc. [798]

3. *Las actividades principales consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.*

Tanto en el literal anterior como en el actual, se menciona la frase a "gran escala". Pero, debido a que no se ha definido el alcance de esta terminología y tampoco un mecanismo numérico que determine su aplicabilidad, el G29 recomienda al responsable o encargado de tratamiento que analice los siguientes factores que permiten identificar si el tratamiento es a gran escala, los cuales son:

> […] el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente; el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento; la duración, o permanencia, de la actividad de tratamiento de datos; el alcance geográfico de la actividad de tratamiento. [799]

El G29 señala como ejemplos de tratamiento a gran escala aquellos que se aplican a: los pacientes en un hospital, las personas que utilizan sistemas de transporte con tarjetas, los clientes de seguros o bancos, los clientes de servicios de entrega con geolocalización, las proveedoras de servicios de telefonía e internet y las empresas de publicidad comportamental. [800]

Aunque son categorías especiales de datos los relacionados a salud y a condenas penales, cuando estos datos estén siendo tratados por un solo médico o abogado, no se entenderán como tratamiento a gran escala, de conformidad con lo señalado por el G29. [801]

4. *De los casos que no se requiere designar DPD*

[798] *Ibíd.*
[799] *Ibíd.*
[800] *Ibíd.*
[801] *Ibíd.*

El G29 señala que si bien pudiera ser obvio que a una organización no requiere la designación de un DPD:

> […] se recomienda que los responsables y encargados del tratamiento documenten el análisis interno realizado para determinar si debe nombrarse o no un DPD, a fin de poder demostrar que se han tenido en cuenta debidamente los factores pertinentes. Este análisis forma parte de la documentación requerida con arreglo al principio de rendición de cuentas. Puede ser exigido por la autoridad de control y debe actualizarse cuando sea necesario, por ejemplo, si los responsables o los encargados del tratamiento llevan a cabo nuevas actividades o prestan servicios nuevos que puedan incluirse en los casos enumerados en el artículo 37, apartado 1". [802]

Respecto del nombramiento del delegado de protección de datos personales, el citado artículo 37 señala las siguientes condiciones que deben cumplirse:

a) Un grupo empresarial podrá nombrar un único delegado de protección de datos, siempre que sea fácilmente accesible desde cada establecimiento.
b) Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.
c) El responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si lo exige la norma de la Unión Europea o la de cada país.

Respecto de aquellos mecanismos organizativos, administrativos y financieros, el artículo 37 del RGPD señala que el delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

Respecto de la designación voluntaria de un DPD, el G29 ha señalado que: "Cuando una organización designe un DPD de forma voluntaria, se aplicarán a su designación, su puesto y sus tareas los requisitos establecidos en los artículos 37 a 39, como si el nombramiento hubiera sido obligatorio". [803]

Finalmente, el responsable o el encargado del tratamiento deberán publicar los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control. Para lo cual deberá tomarse en cuenta lo señalado por el G29 que determina si un responsable o encargado que nombre personal o asesores externos que desempeñen tareas relacionadas con la protección de los datos personales o incluso con el derecho a la intimidad, debe asegurarse que:

[802] *Ibíd.*
[803] *Ibíd.*

> […] que no haya confusión posible con respecto a su cargo, estatus, puesto y tareas. Por ello, debe quedar claro, en cualquier comunicación dentro de la empresa, así como con las autoridades de protección de datos, los interesados y el público en general, que el título de esta persona o asesor no es el de delegado de protección de datos.

Esta aclaración es fundamental, en virtud de que dichas personas carecen de las condiciones de independencia y autonomía que se requiere para la defensa de los derechos de los titulares de los datos y en tal sentido, no cumplen el objetivo de un DPD, por lo que, se debe evitar que sus informes, dictámenes u opiniones causen confusión a lo interno y externo de la institución.

6.12.2 Requisitos para la designación delegado de protección de datos:

Conforme señala el mismo artículo 37 del RGPD, el delegado de protección de datos deberá cumplir con ciertos requisitos que habiliten su designación como:

a) Sus cualidades profesionales.
b) Conocimientos especializados del Derecho y la práctica en materia de protección de datos.
c) Deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente, sean o no empleados del responsable del tratamiento, considerando (97) del RGPD.
d) Capacidad para desempeñar sus funciones.

Aclara este requisito el considerando (97) del RGPD cuando menciona que el nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Es decir, el acervo que le permita resolver cuestiones sobre el tratamiento de una autoridad pública; o el de una del sector privado, o si se trata de operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si el responsable tiene entre sus actividades principales el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales, y no están relacionadas con el tratamiento de datos personales como actividades auxiliares, entre otros que requieren especialización y experticia.

Ahora bien, este requisito ha sido ampliamente cuestionado ya que "la realidad es que no existía una titulación curricularmente homologable al 100% (las más próxima eran las de diversas ramas de informática) y, pese a las solicitudes en ese sentido no se realizó una definición de la figura que incorporase un perfil profesional claro"[804]. Dado que no existe carrera profesional para asumir este trabajo, y debido a que requiere conocimientos especializados, lo obvio es que sea un profesional de cualquier rama el que deba recibir una formación a nivel de postgrado, tomando en cuenta además la responsabilidad de su cargo y su relación directa con las altas gerencias. Por lo que, es posible que cualquier perfil profesional, siempre y cuando tenga

[804] A. RALLO LOMBARTE Y R. GARCÍA MAHAMUT, *Hacia un nuevo derecho europeo de protección de datos*, (Valencia: Tirant lo Blanch, 2015), 560.

conocimiento probado en protección de datos personales, pueda asumir el rol de delegado de protección de datos. Esta conclusión resulta lógica, ya que los actuales tratamientos de datos no tiene un solo enfoque sino que su visión es multidisciplinaria, dado que desde distintas perspectivas se puede obtener valor del dato, por lo que en el dimensionamiento de ese objetivo, el delegado de protección debe velar porque el tratamiento no afecte la dignidad humana y se cumplan las disposiciones establecidas en el RGPD.

Ahora bien, hay autores que sostienen que el perfil del DPD debe ser jurídico, "sin perjuicio de que el delegado de protección de datos sea designado como parte de un equipo multidisciplinar de profesionales, si resulta posible o es conveniente para la organización, que integre también entre otros, a un responsable de seguridad (*Chief Security Officer*, CSO), un oficial de cumplimiento (*Compliance Officer*), al oficial de datos (*Chief Data Officer*, CDO), o incluso a un profesional de relaciones públicas (*Public Relations*, PR)"[805]

Por su parte, la Agencia Española de Protección de Datos ha desarrollado el Esquema de Certificación de Personas para la categoría de "Delegado de Protección de Datos", que tiene el aval de la Entidad Nacional de Acreditación, ENAC, y por el cual, Entidades de Certificación autorizadas, podrán entregar estas certificaciones, siempre y cuando, después de recibir una formación adecuada, proveía por entidades de formación autorizadas, puedan aprobar los requisitos dispuestos.

En dicho esquema consta que el DPD "deberá reunir conocimientos especializados del Derecho y la práctica en materia de protección de datos" y además se ha previsto como requisitos de acceso la necesidad de justificar experiencia profesional en proyectos y/o actividades y tareas relacionadas con las funciones del DPD en materia de protección de datos y también, de ser el caso, formación mínima reconocida en relación con las materias incluidas en el programa del Esquema.[806]

De lo dicho, es evidente que resulta más natural para un perfil profesional abogado el asumir el rol de Delegado de Protección de Datos, pero al haberse construido los requisitos de admisibilidad de forma abierta se permite que otros profesionales, siempre que acrediten experiencia, puedan acceder.

Respecto de si es posible que el responsable de la información designado en virtud del Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, dispuesto en el Real Decreto 3/2010, de 8 de enero español, puede ser nombrado también como delegado de protección de datos personales en el RGPD. El Gabinete Jurídico de la Agencia Española de Protección de Datos señala que:

[805] M. RECIO GAYO, "El delegado de protección de datos", *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, Director: J. Piñar Mañas, (Madrid: Editorial Reus, 2016), 384.

[806] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Esquema de certificación de delegados de protección de datos de la agencia Española de protección de datos, (Esquema AEPD-DPD)*, 13 de junio de 2018, accedido el 16 de noviembre de 2019, .https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf

> […] debe existir la necesaria separación entre el delgado de protección de datos regulado en el RGPD y el responsable de seguridad del ENS, sin que sus funciones puedan recaer en la misma persona u órgano colegiado. Solo excepcionalmente, en aquellas organizaciones que, por su tamaño y recursos, no pudieran observar dicha separación, sería admisible la designación como delegado de protección de datos de la persona que ejerciera las funciones de responsable de seguridad del ENS, siempre que en la misma concurran los requisitos de formación y capacitación previstos en el RGPD. Además, resultaría imprescindible adoptar todas las medidas organizativas, debidamente reflejadas en su Política de seguridad de la información, que garantice la necesaria independencia y la ausencia de conflicto de intereses, por lo que no podría recibir instrucciones respecto al desempeño de sus funciones como delegado de protección de datos, deberá responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. En todo caso, esta circunstancia, que como decíamos, tiene carácter excepcional, deberá evaluarse caso por caso, y deberá dejarse documentada dicha designación haciendo constar los motivos por lo que el organismo correspondiente no ha podido observar dicha separación de funciones así como las medidas que garantizan la necesaria independencia del delegado de protección de datos. [807]

El Esquema establece los requisitos de competencia para la persona que desempeñe el puesto de Delegado de Protección de Datos, así como los criterios para evaluar su posesión por parte de las personas aspirantes, de manera que, cuando el resultado de tal proceso de evaluación sea favorable, la entidad de certificación puede emitir una declaración de cumplimiento o certificado

Llama la atención, la precisión que ha hecho el RGPD al colocar dentro de los requisitos para la designación de un DPD a la necesidad de que tenga capacidades para desempeñar sus funciones. Ya que habitualmente, se debe contratar o vincular personas que puedan cumplir con los perfiles profesionales. Al parecer esta precisión tiene por objeto visibilizar la necesidad de que no solo se consideren habilidades de aquellas consideradas fuertes, relacionadas con la experiencia profesional o la profesionalización, que se analizó previamente, y en las que destacan la formación post-universitaria, las certificaciones y el manejo del idioma inglés, en un nivel alto. Sino que se de prevalencia a aquellas habilidades consideradas suaves, es decir a características personales como la "proactividad, creatividad, asertividad, visión global, capacidad de impacto e influencia, análisis, planificación, formación continua, trabajo en equipo, accesibilidad, transversalidad, empatía y habilidades de comunicación"[808]. Y esto, debido a que, dada la transversalidad del rol de los DPO, quienes deben relacionarse con todas los miembros de una entidad, incluidas las gerencias o altas autoridades, así como con la autoridad de control y también con el titular del dato, esta posición requiere indispensablemente de aptitudes específicas.

[807] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Gabinete Jurídico 170-2018*, accedido el 16 de noviembre de 2019, https://www.aepd.es/media/informes/2018-0170-incompatibilidad-entre-dpd-y-responsable-seguridad.pdf

[808] E. SARACÍBAR , "Una profesión en alza", *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, volumen 76, (2017): 62, accedido el 16 de noviembre de 2019, http://www.redseguridad.com/revistas/red/076/files/assets/basic-html/page-62.html#

Finalmente, debido a la importancia del DPD, la ética profesional resulta ser la característica más importante de este perfil, no solo porque tiene acceso a información confidencial y sensible de la entidad, incluido el modelo de negocio, sino porque si responde a intereses personales, empresariales o de cualquier índole pone en riesgo la supervivencia de la entidad, pero además:

> "[…] una mala praxis del delegado de protección de datos puede suponer un coste excesivo para quien lo ha designado, dado el riesgo de incumplimiento o de crear obstáculos relativos al tratamiento de los datos personales, frenando así, por ejemplo, posibilidades de operación diaria o incluso innovación en una organización".[809]

Es de extrema delicadeza la evaluación del perfil profesional del DPD, por parte del responsable o del encargado de tratamiento, de ahí que este rol debe ser asignado no solo a una persona que sea capaz profesionalmente, con actitudes y aptitudes óptimas, sino y sobre todo, a una persona de probidad notoria.

6.12.3 Funciones del delegado de protección de datos:

El artículo 39 del RGPD señala que el delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) Informar y asesorar al responsable o al encargado y a los empleados que realicen el tratamiento de las obligaciones en virtud del RGPD, de la normativa de la Unión y de cada Estados miembros.
b) Supervisar el cumplimiento de lo dispuesto en el presente del RGPD, de la normativa de la Unión y de cada Estados miembros y "de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes".
c) Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
d) Cooperar con la autoridad de control.
e) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa prevista en el artículo 36
f) Realizar consultas sobre cualquier otro asunto.
g) Desempeñar sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

De las funciones transcritas se desprende que el DPD:

[809] M. RECIO GAYO, *op.cit.,* 376.

> Se trata de una figura que "pivota" entre diferentes departamentos o áreas de la empresa, como pueden ser Recursos Humanos, Seguridad Corporativa, Legal, Marketing, Comercio electrónico, Financiero o Auditoría, esencialmente. El DPD se constituye como el interlocutor del RT o ET con la autoridad de control (que en nuestro país es la Agencia Española de Protección de Datos), de los titulares del derecho a la protección de datos o interesados y de los organismos de certificación, entre otros. (…) El DPD desarrollará funciones de asesoramiento, supervisión, concienciación, formación, cooperación, consulta o interlocución con los interesados.[810]

Sin duda, estas funciones resultan claves para la protección de los titulares de los datos, pero incluso dada la naturaleza del delegado y su conocimiento jurídico tendrá repercusiones en otras aristas y en toda la entidad porque será un vigilante de la garantía de otros derechos humanos, lo que coincide con la visión española que decidió incluir en la normativa de protección de datos personales local a los derechos digitales.

El G29 aclara que "el DPD, ya sea obligatorio o voluntario, se designa para todas las operaciones de tratamiento llevadas a cabo por el responsable o el encargado del tratamiento".[811] En consecuencia, el DPD tiene el derecho a conocer todos los tratamientos de datos personales que esté llevando a cabo la entidad, pero además debe cumplir las funciones, previamente señaladas, en cada uno de estos tratamientos y de esta manera evitar que aquellos riesgosos no sean puestos en su conocimiento.

Asimismo, la directriz del G29 nos permite concluir que la designación voluntaria de un DPD no significa una limitación de competencias. Por el contrario, una vez designado un DPD, no tiene en ningún aspecto, competencia, condición o función diferente a uno que haya sido designado de manera obligatoria, esto por cuanto su objetivo final es proteger el cumplimiento del RGPD.

Resta saber si una vez nombrado un DPD de forma voluntaria, la entidad puede, revocar el nombramiento. Del simple examen, se colige que, como ya señaló el propio G29, si para la no designación de un DPD es necesario un análisis de riesgo documentado que justifique su no necesidad, aún más será obligatorio realizar una revisión, debidamente justificada, que determine que una vez que ha sido nombrado un DPD, e incluso ha estado actuando en funciones, ya no se requiera de esta figura dentro de la organización. Todo lo cual, deberá ser evaluado por la autoridad de control, quien valorará la buena fe de esta actuación institucional, sobre todo, si las actuaciones del DPD cesado estaban causando disgusto a la entidad.

---

[810] R. VELÁZQUEZ, "El delegado de protección de datos en el entorno de la empresa", *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, volumen 76, (2017): 58, accedido el 16 de noviembre de 2019, http://www.redseguridad.com/revistas/red/076/files/assets/basic-html/page-58.html#

[811] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *op.cit. cit.*

El G29, señala que el responsable o el encargado del tratamiento deben recabar el asesoramiento del DPD, respecto de las evaluaciones de impacto relativas a la protección de los datos:

> […] si debe llevarse a cabo o no una evaluación de impacto relativa a la protección de datos; qué metodología debe seguirse al llevar a cabo una evaluación de impacto; si debe realizarse la evaluación de impacto en la propia organización o subcontratarse; qué salvaguardias (incluidas medidas técnicas y organizativas) deben aplicarse para mitigar cualquier riesgo para los derechos e intereses de los interesados; si la evaluación de impacto relativa a la protección de datos se ha llevado a cabo correctamente o no y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardias aplicar) son conformes con los requisitos de la protección de datos.[812]

El asesoramiento a la evaluación de impacto debe ser integral. El G29 al precisar los ámbitos de intervención y asesoría que el DPD debe realizar, clarifica sus funciones. Las cuales deben cumplirse y con ello evitar discrecionalidades, tanto del responsable como encargado de tratamiento que, por ejemplo, no ponga en conocimiento del DPD ciertos tratamientos. Así como, del propio delegado que no debe eludir pronunciarse de todo cuanto represente un tratamiento de datos personales en una entidad, desde todos los enfoques o aristas posibles.

En el caso de la normativa española, se establece funciones adicionales a los DPD ya que:

> […] el artículo 37 LOPDGDD contempla la intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos configurándola como una instancia previa obligatoria. No olvidemos que también está prevista la participación del DPD en la notificación de violaciones de seguridad y en el trámite de consulta previa entre otros.[813]

Como vemos, se otorga en la legislación española al DPD se le otorga un rol reforzado por cuanto la autoridad de control se ayuda de esta figura para solucionar de primera mano los reclamos de los titulares y en solo caso de que no se satisfaga los requerimientos del titular, se podrá reclamar ante la autoridad de control. De esta manera, resulta más eficiente y ágil el sistema de protección. Así mismo, se le otorga un rol más activo al determinar que sea el DPD quien notifique las violaciones de seguridad, con lo cual se intenta evitar que las entidades por cuestiones de credibilidad e imagen omitan el cumplimiento de esta obligación. En el mismo sentido, "puede desempeñar un papel importante en la elaboración, y mantenimiento, del registro de las actividades del tratamiento, previsto en el artículo 30 del Reglamento como obligación que corresponde al responsable de tratamiento"[814]

6.12.4 Garantías de autonomía e independencia del delegado de protección de datos:

[812] *Ibíd.*
[813] R. MARTÍNEZ, *op.cit.*
[814] M. RECIO GAYO, *op.cit*., 384.

Conforme señala el artículo 38 del RGPD el responsable y el encargado del tratamiento garantizarán el ejercicio de las funciones del delegado de protección de datos y que estas funciones y cometidos no den lugar a conflicto de intereses y además lo respaldarán a través de las siguientes acciones:

a) Permitirle participar de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales. Si bien, la norma no lo señala, es necesario acotar que es obligación del delegado de protección de datos realizar acciones tendientes a exigir esta participación, todo desde la perspectiva de la responsabilidad en sus funciones y sus deberes proactivos.
b) Facilitar los recursos necesarios para el desempeño de sus funciones.
c) Facilitar el acceso a los datos personales y a las operaciones de tratamiento.
d) Facilitar el mantenimiento de sus conocimientos especializados.
e) Garantizar que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones.
f) No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones.
g) Cumplir con que el delegado de protección de datos rinda cuentas directamente al más alto nivel jerárquico del responsable o encargado. Nuevamente el delegado de protección debe buscar aun sin apoyo realizar esta acción en cumplimiento de sus deberes y responsabilidades propias.
h) Permitir que los interesados puedan ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del Reglamento. El delegado de protección también tiene un deber de buscar medios que le permitan cumplir con este objetivo, aun sin el apoyo de los responsables y encargados, pero además podrá solicitar a la autoridad de control que intervenga para que estas obligaciones se cumplan, todo esto aunque no está desarrollado expresamente en la norma, sin embargo debe realizarse desde el enfoque de responsabilidad proactiva.
i) Respetar la obligación del delegado de protección de datos de mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones.
j) Permitirle al delegado de protección de datos desempeñar otras funciones y cometidos.

Sin duda, una de las garantías más importante de independencia y autonomía del DPD persona física:

> […] que no puede ser removido ni sancionado por el responsable o el encargado por el desempeño de sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio. Por lo tanto, el despido que se produzca en el ejercicio de sus funciones debe entenderse nulo de pleno derecho (garantía de indemnidad) salvo que, como en el caso de los representantes de los trabajadores, se trate de un despido disciplinario conforme a lo previsto en el art. 54 del ET.[815]

De lo citado, para que la remoción de un PDP pueda considerarse válida, las actuaciones que motivaron su separación deberán enmarcarse en el dolo o la negligencia grave. Ahora bien, esta situación, conforme señalan algunos autores, se considera:

[815] E. SIERRA BENÍTEZ, *op.cit. cit*., 258.

> […]una severa limitación al poder disciplinario del empresario puesto que en los supuestos de pérdida de confianza como consecuencia del ejercicio irregular del cargo, tendría que demostrarse tanto el dolo o la negligencia del DPD como la gravedad de la conducta para imponer una medida disciplinaria procedente. Así, una interpretación estricta de la previsión del Anteproyecto podría conllevar supuestos en los que el DPD haya perdido temporal o definitivamente la certificación obtenida para el ejercicio del cargo, y sin embargo no pueda ser despedido de forma procedente al no quedar acreditado el dolo o negligencia o la gravedad de la conducta, puesto que, como se observó en el apartado 2.3. el régimen disciplinario de las entidades certificadoras no exige dicha prueba.[816]

De lo transcrito, se colige que será la normativa y la jurisprudencia la que vaya delineando la respuesta a este vacío normativo que, si bien pretende otorgar indemnidad al DPD para el ejercicio libre de su cargo, también representa un riesgo, ya que una actuación negligente que sin ser considerada grave, en la práctica, puede significar un deterioro paulatino para el funcionamiento y la debida organización de la entidad.

El artículo 35 de la LOPDGDD española señala que los DPD podrán ser personas naturales o jurídicas. Si bien el RGPD no menciona la característica de que el DPD sea una persona jurídica resulta interesante el desarrollo español, toda vez que puede ser un mecanismo eficiente para garantizar la independencia en los pronunciamientos y asesoramientos que realicen, ya que estaría en riesgo la credibilidad de estas personas jurídicas cuya finalidad sería precisamente brindar este tipo de servicios a varias entidades. En consecuencia, para mantener su reputación y relación adecuada con la autoridad de control resulta evidente que deben cumplir un verdadero rol de garante de los derechos.

Otra garantía de eficiencia que repercute en la independencia, es aquella que señala la normativa española sobre los criterios de permanencia del delegado, toda vez que el artículo 34 numeral 5 de la misma normativa determina que la dedicación puede ser completa o a tiempo parcial, "en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados".

Como garantía de oportunidad, el artículo 36 numeral 3 de la LGPDPGDD señala que el DPD tendrá acceso a todos los datos personales y procesos de tratamiento sin que le sea oponible la existencia de cualquier deber de confidencialidad o secreto.

6.13 Transferencia internacional de datos

[816] H. MONZÓN PÉREZ, *La naturaleza de la relación laboral del "Delegado de Protección de Datos"*, *IUSLabor*, volumen 2, (2017), 19.

El considerando (101) del RGPD reconoce la necesidad del intercambio transfronterizo de datos personales entre la Unión Europea y los Estados miembros con terceros países u organismos internacionales, ya que son necesarios para la expansión del comercio y la cooperación internacionales, pero además representan una realidad inevitable de carácter mundial que presenta dificultades, sobre todo, en lo que respecta a la protección de los datos de carácter personal. Esta situación debe ser asumida como un reto, pues no es posible ceder ante el respeto que todos los seres humanos merecemos a nuestra dignidad humana y en consecuencia a los derechos humanos. Por eso, se establece el RGPD como un estándar de protección que debe ser respetado, sin perjuicio de los acuerdos internacionales celebrados o que pudieran celebrarse, incluidas las garantías para los interesados y las obligaciones resultantes de la participación del tercer país u organización internacional en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, y el cumplimiento de esas obligaciones (considerando [105], RGPD), siempre y cuando establezcan un nivel adecuado a vista del Reglamento (considerando [102], RGPD).

El capítulo V del RGPD establece el sistema de transferencias de datos personales a terceros países u organizaciones internacionales, para lo cual determina el principio general que rige las transferencias como criterio básico, uniforme y de aplicación general, que en consecuencia organiza y orienta este sistema.

El citado régimen de transferencia internacional de datos se organiza desde la perspectiva de aquellos países que cumplen niveles adecuados de protección, que a criterio del RGPD son los establecidos en esta normativa, que se considera el mayor estándar de protección.

Se establecen, entonces, mecanismos de transferencias que buscan determinar los medios para lograr una transferencia internacional de datos adecuada, los cuales son:

a) Transferencias basadas en una decisión adecuada.
b) Transferencias mediante garantías adecuadas.
c) Normas corporativas vinculantes.
d) Excepciones para situaciones específicas.
e) Transferencias sin el amparo de mecanismos transfronterizos de datos a terceros países.

Adicionalmente, este régimen de protección establece aquellas transferencias o comunicaciones no autorizadas por el derecho de la Unión y los mecanismos de cooperación internacional en el ámbito de la protección de datos transfronterizos a terceros países como mecanismo de clausura que pretende regular por completo esta temática compleja, no solo desde la perspectiva técnica, que en muchos casos dificulta sobre todo el control, sino jurídica porque atiende al ideal de universalizar el estándar europeo como hegemónico en el mundo, desde la perspectiva de que es el que da mayores garantías para el ser humano, como centro de todo desarrollo tecnológico, social, económico y cultural.

6.13.1 Principio general de las transferencias

El artículo 44 del RGPD, con la finalidad de asegurar que se cumpla un nivel adecuado de protección de las personas físicas, establece el principio general de las transferencias.

Este principio, aplicable a los datos transfronterizos que se remitan a terceros países, dispone que únicamente se autorizará la transferencia de datos personales a un tercer país u organización internacional, si su tratamiento durante y después de la llegada a destino cumple las siguientes condiciones ineludibles:

a) el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el capítulo V del RGPD;
b) se respetan las condiciones del RGPD, inclusive para transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional.

Este principio es un mecanismo fáctico que busca la aplicación extraterritorial del RGPD, en especial de aquellas condiciones esenciales que permiten la vigencia del derecho a la protección de datos personales en países donde no existe normativa que proteja a la persona. Tomando en cuenta que la sociedad de la información es global y que los esfuerzos aislados de protección o los sistemas de autorregulación no son suficientes pues no permiten garantizar los derechos de las personas físicas. El sistema de transferencias internacionales de datos personales se convierte en una herramienta útil para intentar disminuir los riesgos a los derechos fundamentales, pues busca aplicar un nivel adecuado de protección entre países y por ende una uniforme aplicación de la normativa que permia la garantía de los derechos.

6.11.2 Cooperación internacional en el ámbito de la protección de datos personales

Al tenor del artículo 50 del RGPD, para facilitar la aplicación eficaz de la legislación sobre protección de datos personales, las garantías adecuadas y los derechos y libertades fundamentales, y mejorar la relación entre terceros países, organizaciones internacionales y la Comisión y las autoridades de control de los Estados miembro, sobre todo para garantizar a las personas cuyos datos personales circulan a través de las fronteras hacia el exterior de la Unión y que suponen en mayor riesgo de daño y dificultades para el ejercicio de los derechos de protección de datos (considerando [116], RGPD), se tomarán medidas apropiadas como las siguientes:

a) Crear mecanismos de cooperación internacional.
b) Prestarse mutuamente asistencia a escala internacional, en particular mediante:

    a. La notificación de reclamaciones.
    b. La remisión de reclamaciones.
    c. La asistencia en las investigaciones
    d. El intercambio de información

c) Asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional y la aplicación de la normativa de protección.
d) Promover el intercambio y la documentación de la legislación y de prácticas, inclusive en materia de conflictos de jurisdicción con terceros países.

6.13.3 Transferencias basadas en una decisión de adecuación

Es un mecanismo de transferencia fronteriza de datos, reconocido en el considerando (103) y en el artículo 45 del RGPD, por el cual la Comisión como máximo organismo encargado de velar la vigencia y aplicación del RGPD, verifica y califica si un tercer país, territorio, uno o varios sectores específicos de ese tercer país, o la organización internacional tiene un nivel adecuado de protección de los datos personales, mediante una decisión de adecuación recogida en un acto de ejecución.

Obtenida la autorización de la Comisión, estas transferencias internacionales no requerirán de autorización específica.

1. Evaluación de nivel adecuado

Para que la Comisión pueda evaluar en qué consiste un nivel de protección adecuado, se tomará en cuenta varios de los elementos que desde el contexto normativo y desde la aplicación real, incluidos los mecanismos de supervigilancia y control, ostenta un país para la vigencia de este derecho.

Estos elementos ineludibles, porque no pueden ser soslayados, ya que de no existir impiden la autorización de transferencia, son:

a) *Respeto a las libertades individuales y a los derechos fundamentales*

Para la evaluación de un estado con la consideración de nivel adecuado se requiere demostrar que en él existen garantías para asegurar el respeto a la dignidad humana como base para la protección de los derechos humanos, entre ellos el derecho a la protección de datos personales. Es decir, que se trata de un país en el que se vive en un Estado de derecho,

Asimismo, se entiende con nivel adecuado los países en los que existe normativa específica, pertinente, tanto general como sectorial sobre protección de datos personales, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales. Así como, normativa relativa a secreto profesional, medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización

internacional. Pero no solo es suficiente la existencia de normativa sino que es necesario que esta se aplique.

Asimismo, otra evidencia de que un estado maneja un nivel adecuado de respeto a las libertades individuales y a los derechos fundamentales es la que hace referencia a la puesta a disposición del titular de datos de herramientas de exigibilidad de sus derechos, tanto en el ámbito administrativo como en el judicial. De esta forma, los tribunales del tercer país y por ende su jurisprudencia reconocen el derecho de acción, así como la tutela judicial efectiva una vez iniciado un proceso, garantizando el cumplimiento de las garantías procesales.

b) *Autoridades de control independientes*

La normativa de protección de datos resulta ineficiente sino puede ser exigible, para ello es fundamental la existencia y funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional.

Estas instituciones deben cumplir a cabalidad y con responsabilidad su misión de asistir y asesorar a los interesados en el ejercicio de sus derechos, construir en sumo una cultura de protección. Pero, sobre todo, la entidad de control del tercer país debe garantizar y hacer cumplir las normas en materia de protección de datos. Ante todo, es indispensable que pueda responder a los requerimientos que plantea el RGPD, esto es los poderes públicos de investigación, correctivos, de autorización y consultivos que constan en el artículo 58 del RGPD. Ya que solo en la asistencia mutua y en la cooperación de las distintas entidades que protegen a escala internacional los datos personales se puede garantizar una real protección de los titulares.

c) Compromisos internacionales

Si no existe normativa internacional como son tratados, convenios, pactos, instrumentos de cooperación, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, no será posible transferencia de datos personales. Ya que no se tratan de estados que manejen un nivel adecuado de protección. Por lo que, la participación de los países en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, de los cuales el tercer país u organización internacional sea parte o beneficiario, demuestran que existe el compromiso de un Estado de adaptar su normativa, su institucionalidad, sus políticas públicas; en suma todas las condiciones necesarias para la implementación real en un Estado.

2. Procedimiento de la Comisión para emitir una decisión de adecuación

Para emitir una decisión de adecuación se seguirá el siguiente procedimiento:

a) La Comisión evaluará la adecuación del nivel de protección, utilizando los criterios antes analizados.
b) La Comisión dictará un acto de ejecución en el que afirmará que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantiza un nivel de protección adecuado.
c) El acto de ejecución establecerá:

    a. Un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El considerando (106) del RGPD señala que para esta revisión, la Comisión debe tomar en consideración las opiniones y conclusiones del Parlamento Europeo y del Consejo, así como de otros organismos y fuentes pertinentes, y evaluar, en un plazo razonable, la aplicación de dichas decisiones e informar al Comité.
    b. El ámbito de aplicación territorial y sectorial.
    c. Determinará la autoridad o autoridades de control competente.

d) La Comisión supervisará de manera continua los acontecimientos en países terceros y organizaciones internacionales que puedan afectar el acto de ejecución que dictamina un nivel adecuado.
e) La Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión si no se garantiza un nivel de protección adecuado. El considerando (107) del RGPD señala que debe prohibirse la transferencia de datos personales a un tercer país u organización internacional, que no cumplan los requisitos del RGPD si no existen garantías adecuadas, incluidas las normas corporativas vinculantes, ni excepciones aplicadas a situaciones específicas. En ese caso, debe realizar consultas entre la Comisión y esos terceros países u organizaciones internacionales a fin de subsanar la situación.
f) El acto de ejecución de emisión como el de revocatoria se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2 del RGPD.
g) La Comisión adoptará actos de ejecución inmediatamente aplicables en casos de urgencia (art. 93, apdo. 3, RGPD).
h) La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la inadecuada protección.
i) La Comisión publicará en el *Diario Oficial de la Unión Europea* y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

6.13.4 Transferencias mediante garantías adecuadas

Es un mecanismo de transferencia transfronteriza de datos reconocido en el considerando (103) y en el artículo 46 del RGPD, que opera cuando no existe una decisión de adecuación recogida en un acto de ejecución dictado por la Comisión, de conformidad con el artículo 45, numeral 3.

El considerando (108) del RGPD señala que a falta de decisión de adecuación, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país, mediante garantías adecuadas para el interesado.

1. Concepto de garantías adecuadas

Al tenor del considerando (108) y del artículo 46 del RGPD, se entienden por garantías adecuadas aquellas características indispensables, que facultan a dos países a realizar transferencias internacionales de datos personales. Esto se debe a que los responsables o encargados del tratamiento pueden transmitir datos personales siempre y cuando cumplan con las siguientes condiciones:

a) La observancia de requisitos de protección de datos, adecuados al tratamiento dentro de la Unión.
b) El respeto por los derechos de los interesados, adecuados al tratamiento dentro de la Unión.
c) Derechos exigibles y acciones legales efectivas a disponibilidad de los interesados.
d) El derecho a obtener una reparación administrativa o judicial efectiva.
e) El derecho a reclamar una indemnización, en la Unión o en un tercer país.
f) El cumplimiento de los principios generales relativos al tratamiento de los datos personales.
g) El cumplimiento de los principios de protección de datos desde el diseño y por defecto.

2. Mecanismos que demuestran garantías adecuadas en un tercer país u organización cuando no cuentan con autorización de la autoridad de control

De conformidad con el citado artículo 46, las garantías adecuadas pueden ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control mediante:

a) Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.
b) Normas corporativas vinculantes (art. 47, RGPD).
c) Cláusulas tipo de protección de datos adoptadas por:

    a. La Comisión de conformidad con el procedimiento de examen (art. 93, apdo. 2, RGPD).
    b. Una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen (art. 93, apdo. 2, RGPD).
    c. Inclusión de cláusula tipo en contratos más amplios, la existencia de cláusulas tipo de protección de datos adoptadas por la Comisión o autoridad de control no debe obstar a que los responsables o encargados incluyan estas cláusulas tipo en un contrato más amplio; por ejemplo, un contrato entre dos encargados (considerando [109], RGPD).
    d. Cláusulas o garantías adicionales. Se alentará a responsables y encargados del tratamiento a ofrecer garantías adicionales mediante compromisos

contractuales que complementen las cláusulas tipo de protección de datos, siempre que no contradigan, directa o indirectamente, o mermen los derechos o las libertades fundamentales de los interesados (considerando [109], RGPD).

d) Un código de conducta aprobado (art. 40, RGPD), junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados.
e) Mecanismo de certificación (art. 42), junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados.

3. Mecanismos que demuestran garantías adecuadas en un tercer país u organización cuando cuentan con autorización de la autoridad de control

Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a) Cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional.
b) Acuerdos administrativos, si la transferencia es entre autoridades públicas o con organizaciones internacionales con competencias, pero con autorización de la autoridad de control (considerando [108], RGPD).
c) Disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.
d) Memorando de entendimiento, si la transferencia se realiza entre autoridades o entidades públicas con entidades o autoridades públicas de terceros países o con organizaciones internacionales con competencias o funciones correspondientes, pero con autorización de la autoridad de control (considerando [108], RGPD).
e) La autoridad de control aplicará el mecanismo de coherencia, de ser necesario (art. 63, RGPD).

Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de o por la Comisión, anteriores a la vigencia del RGPD, permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas de conformidad con los actuales procedimientos descritos.

6.14.5 Normas corporativas vinculantes

El considerando (110) del RGPD señala una figura propia de los grupos empresariales o de la unión de empresas de actividad económica conjunta, denominado normas corporativas vinculantes, que les permita un trabajo coordinado, armónico, coherente entre las distintas organizaciones que las conforman respetando los principios esenciales y derechos aplicables que otorguen garantías adecuadas para las transferencias.

Es un mecanismo de transferencia transfronteriza de datos, reconocido en el artículo 47 del RGPD, dictado por la autoridad de control competente en aplicación de un mecanismo de coherencia, reconocido en el artículo 63 del RGPD.

1. Aprobación de normas corporativas vinculantes

La autoridad de control competente aprobará normas corporativas vinculantes cuando estas sean:

a) Jurídicamente vinculantes, se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados (art. 47, RGPD).
b) Confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales (art. 47, RGPD).
c) Cumplan los requisitos establecidos en el apartado 2. 2 del artículo 47; es decir, apliquen las normas corporativas mínimas que deben constar en las normas corporativas vinculantes, conforme se analizará a continuación.

2. Contenido mínimo de las normas corporativas vinculantes

Las normas corporativas vinculantes especificarán, como mínimo, los siguientes elementos:

a) Datos de contacto
   a. La estructura del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta.
   b. Los datos de contacto de cada uno de sus miembros.

b) Las transferencias o conjuntos de transferencias de datos
   a. Categorías de datos personales.
   b. Tipo de tratamientos.
   c. Fines del tratamiento.
   d. Tipo de interesados afectados.
   e. Nombre del tercer o los terceros países.

c) La aplicación de los principios generales en materia de protección de datos
   a. Licitud y lealtad.
   b. Finalidad explícita y legítima.
   c. Adecuados y pertinentes.
   d. No excesivos en relación con los fines para los que son tratados, limitación de la finalidad.
   e. Calidad de los datos: exactos y actualizados.
   f. Períodos de conservación limitada.
   g. Minimización de los datos.
   h. Protección de los datos desde el diseño y por defecto.
   i. La base del tratamiento.
   j. El tratamiento de categorías especiales de datos personales.

k. Las medidas encaminadas a garantizar la seguridad de los datos.
l. Los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes.

d) Los derechos de los interesados y los medios para ejercerlos

a. En relación con el tratamiento.
b. A no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad, con lo dispuesto en el artículo 22 del RGPD.
c. El derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros, de conformidad con el artículo 79 del RGPD.
d. El derecho a obtener una reparación.
e. El derecho a una indemnización por violación de las normas corporativas vinculantes, cuando proceda.
f. Los procedimientos de reclamación.

e) Cláusula de responsabilidad

a. La aceptación de la responsabilidad por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión.
b. Exoneración del responsable o el encargado, solo será exonerado, total o parcialmente de la responsabilidad, si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro.

f) Información al interesado

Es decir, la forma en la que se facilita a los interesados la siguiente información:

a. La existencia de normas corporativas vinculantes.
b. Aplicación de principios generales (art. 47, num. 2, lit. d), RGPD).
c. Los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos (art. 47, num. 2, lit. e), RGPD).
d. Información que deberá facilitarse cuando los datos personales se hayan obtenido del interesado (art. 13, RGPD).
e. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado (art. 14, RGPD).
f. El carácter jurídicamente vinculante de las normas corporativas, tanto a nivel interno como externo.

g) Mecanismos de supervisión del cumplimiento de las normas vinculantes

a. Las funciones del delegado de protección de datos designado o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta.
b. La supervisión de la formación.
c. La supervisión de la tramitación de las reclamaciones.

h) Mecanismos de verificación del cumplimiento de las normas vinculantes

a. Los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes.
b. Auditorías de protección de datos.
c. Métodos para garantizar acciones correctivas para proteger los derechos del interesado.
d. Comunicar los resultados de la verificación a la persona o entidad que ejerce la supervisión del cumplimiento de las normas vinculantes (ver ítem inmediato anterior).
e. Comunicar los resultados de la verificación al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta.
f. Ponerse a disposición de la autoridad de control competente que lo solicite.

i) Mecanismos de comunicación a la autoridad de control

a. Para comunicar las modificaciones introducidas en las normas.
b. Para registrar las modificaciones introducidas en las normas.
c. Para notificar las modificaciones introducidas en las normas a la autoridad de control.

j) Mecanismos de cooperación con la autoridad de control

a. Para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta.
b. Poner a disposición de la autoridad de control los resultados de los mecanismos de verificación del cumplimiento de las normas vinculantes.

k) Mecanismos para informar a la autoridad de control de cualquier requisito jurídico de aplicación, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes

a. En un país tercero a un miembro del grupo empresarial.
b. De la unión de empresas dedicadas a una actividad económica conjunta.

l) La formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

m) Intercambio de información

a. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes.
b. Los actos de ejecución dictados por la Comisión se adoptarán con arreglo al procedimiento de examen (art. 93, apdo. 2, RGPD).

6.15.6 Transferencias o comunicaciones no autorizadas por el derecho de la Unión

El considerando (115) y el artículo 48 del RGPD señalan que no se podrá autorizar transferencias o comunicaciones de datos personales por parte de responsables o encargados regidos por el RGPD a terceros países, incluso si esta transferencia se solicita mediante

sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país.

Únicamente será reconocida o ejecutable en cualquier modo la citada sentencia o la decisión de autoridad administrativa de un país si existe un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro.

Esta salvedad, constante en el RGPD, intenta evitar que se puedan usar otras jurisdicciones para evadir las responsabilidades impuestas por el Reglamento, o en su defecto obtener datos de personas interesadas protegidas por esta normativa utilizando en abuso del derecho, normativa y justicia de un tercer país. Tiene sentido, además, pues para que un tercer país u organización pida información, aun a título de sentencia judicial, se debe revisar primero su adecuación, de tal forma que el requerimiento de un tratado viene a suplir esta revisión.

6.16.7 Excepciones para situaciones específicas

El considerando (111) y el artículo 49 del RGPD señalan varias situaciones específicas que, pese a no existir una decisión de adecuación aprobada por la Comisión, tampoco garantías adecuadas presentadas por el responsable o el encargado o una autoridad de control, ni aún normas corporativas vinculantes, se puede realizar una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente si se cumple alguna de las condiciones siguientes que se va a analizar.

1. *Condiciones para transferencias de datos a terceros países en los casos de excepciones para situaciones específicas*

    a) Consentimiento explícito del interesado
    a. Información previa de los posibles riesgos para el titular por no existir decisión de adecuación y de garantías adecuadas.
    b. El interesado consiente explícitamente.
    c. Esta excepción no será aplicable a actividades realizadas por autoridades públicas en el ejercicio de sus poderes públicos.

    b) Celebración y ejecución de un contrato entre interesado y responsable de tratamiento
    a. La transferencia es necesaria para la celebración de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica.
    b. La transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento, a solicitud del interesado.
    c. No será aplicable a actividades realizadas por autoridades públicas.

    c) Ejecución de medidas precontractuales entre interesado y responsable de tratamiento

a. La transferencia es necesaria para la ejecución de medidas precontractuales adoptadas a solicitud del interesado.
b. No será aplicable a autoridades públicas.

d) Interés público

a. La transferencia sea necesaria por razones importantes de interés público.
b. El interés público será reconocido por el derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
c. El considerando (112) del RGPD establece que se entiende como casos de interés público, los intercambios internacionales de datos entre autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública; por ejemplo, en caso de contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte.

e) Ejercicio de reclamaciones

La transferencia sea necesaria para:

a. La formulación de reclamaciones.
b. El ejercicio de reclamaciones.
c. La defensa de reclamaciones.

f) Intereses vitales

Se permite en dos casos:

a. La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas.
b. El interesado esté física o jurídicamente incapacitado para dar su consentimiento.

g) Registro público

Se facilita en los siguientes supuestos:

a. Se realice desde un registro público que tenga por objeto facilitar información al público.
b. El registro público esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo; en este último caso, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.
c. Es necesario que en cada caso particular, se cumplan las condiciones que establece el RGPD y la normativa interna de cada Estado miembro para la consulta.
d. No abarcará la totalidad de los datos personales.
e. No abarcará categorías enteras de datos personales contenidos en el registro.

6.17.8 Requisitos para la transferencia de datos a terceros países a los que no les ampara ningún mecanismo transfronterizo de datos a terceros países

El considerando (113) y el artículo 49, numeral 1, párrafo final, del RGPD señalan los requisitos para la transferencia de datos a terceros países a los que no les ampara ni una decisión de adecuación aprobada, ni garantías adecuadas, ni corporativas vinculantes, ni aun los casos de excepción específica, y solo deben ser posibles en "casos aislados, cuando ninguno de los otros motivos para la transferencia sean aplicables".

Solo podrá llevarse a cabo esta transferencia que no tiene ningún tipo de amparo, a riesgo de responsable de tratamiento:

a) Sobre tratamiento

a. Si no es repetitiva.
b. Afecta solo a un número limitado de interesados.
c. Es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento, siempre y cuando no prevalezcan los intereses o derechos y libertades del interesado. El considerando (47) de RGPD señala que se entiende por interés legítimo una relación pertinente y apropiada entre el interesado y el responsable, como la del interesado como cliente o está al servicio del responsable garantizar la seguridad de la red y de la información, las de marketing directo, e incluso para fines administrativos internos; en todo caso este interés será meticulosamente revisado.
d. No será aplicable por autoridades públicas, puesto que es indispensable que exista un ley como base jurídica para el tratamiento de datos personales por parte de las autoridades públicas (considerando [47], RGPD).

b) Sobre obligaciones del responsable

a. El responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos.
b. Sobre la base de una evaluación de impacto el responsable del tratamiento ofrece garantías apropiadas con respecto a la protección de datos personales.
c. El responsable del tratamiento debe informar obligatoriamente a la autoridad de control de la transferencia.
d. El responsable del tratamiento entregará la información que deberá facilitarse cuando los datos personales se obtienen del interesado (art. 13).
e. El responsable del tratamiento entregará la información que deberá facilitarse cuando los datos personales no se obtienen del interesado (art. 14).
f. El responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.
g. El responsable o el encargado del tratamiento documentarán en los registros de actividades de tratamiento para su evaluación y las garantías (art. 30, RGPD).
h. Aunque la Comisión no haya dictado acto de ejecución sobre el nivel adecuado de la protección de datos en un tercer país, el responsable o el encargado del tratamiento están obligados a arbitrar soluciones que faciliten

a los interesados sus derechos, incluso en transferencias posteriores de forma que los titulares sigan gozando de los derechos fundamentales y garantías (considerando [114], RGPD).

7. Contenido esencial del derecho a la protección de datos personales en Europa

El camino que ha transitado el derecho a la protección de datos en Europa ha sido producto de una concienciación paulatina, cuyo resultado necesariamente debía ser el nacimiento de un nuevo derecho humano, fundamental e inminente en la era digital, denominado derecho a la protección de datos personales. Únicamente de esta forma se puede garantizar a las personas una protección eficaz ante las diversas y cada vez más sofisticadas formas de trasgresión que se suscitan por los avances tecnológicos.

La protección de los datos personales limitada a una manifestación del derecho a la intimidad no podía mantenerse por mucho tiempo, porque aunque se pretendía concebirla, en un sentido muy amplio como el que nos evoca la *privacy*, y de esta forma extenderla a todo tipo de información personal, incluyendo aquellos datos que no son de carácter íntimo sino privado e incluso social. Sin embargo, era insuficiente para proteger aquellos datos personales considerados inocuos y que pueden ser sometidos a procesos automatizados para otorgar perfiles completos de la personalidad de un individuo. Porque la utilización de los datos personales no solo afecta la esfera de la privacidad o su derecho a la intimidad y a la vida privada o a los derechos asociados directamente a la personalidad del individuo como el derecho a la imagen y a la voz, el derecho a la honra, el derecho a la identidad, sino que las transgresiones al tratamiento de datos personales pueden provocar casos de discriminación y llegarse incluso a conculcar otros derechos fundamentales como la salud, el trabajo, la vivienda, la educación. Pero, además, el tratamiento inadecuado de datos puede llegar a afectar derechos reales y de crédito debido, por ejemplo, a la inexactitud, imprecisión o desactualización de las datos personales.

El derecho a la protección de datos personales ha partido de un derecho pasivo de primera generación que proclamaba la "no injerencia en la vida privada" del individuo,[817] a uno de tercera generación, el de la libertad informática, esto es a un nuevo derecho del individuo a tutelar su propia identidad informática, concretándose las garantías del acceso y control de las informaciones procesadas en bancos de datos por parte de las personas a las que concierne.[818]

La autodeterminación informativa es el corazón del derecho a la protección de datos personales, porque le permite a la persona, desde una postura activa, empoderarse de sus datos, controlarlos, y decidir sobre su uso, autorización y cesión para su tratamiento, hasta su defensa mediante otros derechos como: el de acceso, rectificación, supresión, oposición, limitación al tratamiento,

[817] F. SARDINA VENTOSA, "El derecho a la intimidad informática y el tratamiento de datos personales para la prevención del fraude", *Actualidad Informática Aranzadi: revista informática para juristas* (1997). accedido 15 de junio del 2007, http://intra.pre.gva.es/convera/docpdf_castellano/articulosrevista/13a16/sardinaventosa97.pdf
[818] A. PÉREZ LUÑO, *Manual de Informática* (Barcelona: Ariel, 1996), 1.

no discriminación por procesamientos automatizados, entre otros, y de sus correspondientes mecanismos de tutela efectivos.

En Europa se ha dictado normativa para la protección de personas en relación al tratamiento de sus datos personales desde 1950,[819] y desde ese entonces ha evolucionado, desde una salvaguarda limitada a la intimidad hasta uno basado en un derecho fundamental independiente y autónomo, denominado protección de datos personales, que exige un sistema de protección integral y completo, dinámico, en constante crecimiento, que intenta responder directamente a los avances tecnológicos y que consta en el Reglamento de Protección de Datos Personales (RGPD).[820]

Esa normativa plantea el estándar mundial de protección, considerado el más alto, porque permite el libre flujo informacional y, al mismo tiempo, plantea una serie de requisitos, condiciones y tutelas en garantía de los derechos fundamentales de las personas. Su aplicación es directa en aquellos países que forman parte de la Unión Europea y en aquellos que guarden relación con esta, ya sea porque ofrezcan bienes o servicios, porque traten datos de sus residentes o porque uno de sus establecimientos se encuentra en su territorio.

Al tenor del considerando (13) del RGPD, este instrumento tiene por objetivo:

> [...] para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros.

El mayor reto que plantea esta normativa es el justo equilibrio entre la libre circulación de los datos personales y la protección de los datos de las personas naturales. Esto debido a que para la mejora de los servicios públicos, la implementación del gobierno de la información, la simplificación de trámites, el crecimiento del mercado, el desarrollo de las empresas, de los servicios, el impulso de la innovación, del avance científico y tecnológico es indispensable el uso de datos personales; por eso su flujo y tratamiento no debe ser restringido, ni prohibitivo.

---

[819] CONVENIO PARA LA PROTECCIÓN DE LOS DERECHOS HUMANOS Y DE LAS LIBERTADES FUNDAMENTALES, de Roma

[820] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), Documento DOUE-L-2016-80807.

Ahora bien, no se puede sacrificar las libertades individuales, los derechos fundamentales e incluso otros derechos reales y de crédito, en aras de las mejoras económicas, sociales y tecnológicas. Es en este sentido que esta circulación encuentra la limitación que la normativa europea intenta construir sobre la base de una serie de requisitos, condiciones, derechos, principios con los que garantiza un uso legal, pero sobre todo legítimo, de buena fe, diligente y proactivo del tratamiento y uso por parte de responsables y encargados públicos y privados de los datos personales.

Otra de las cuestiones que deben ser visibilizadas es aquella relativa a las condiciones propias de las microempresas y las pequeñas y medianas empresas, para las cuales es necesario establecer un régimen especial que les permita competir con otras grandes empresas sin que la aplicación de esta normativa les signifique una desventaja comparativa que impida su surgimiento. Por eso, se ha previsto, por ejemplo, "una serie de excepciones en materia de llevanza de registros para organizaciones con menos de 250 empleados" (considerando [13], RGPD).

Situación especial amerita la igualdad como condición básica para la aplicación del RGPD, ya que todos los responsables o encargados del tratamiento deben someterse y aplicar esta normativa, sin excepción que pueda significar una ventaja competitiva. De otro lado, la igualdad también debe ser dirigida a que se debe garantizar "un nivel equivalente de protección de las personas físicas y la libre circulación de datos personales en la Unión Europea" (considerando [170], RGPD).

Como los casos, las problemáticas y las situaciones de justificación o excepción para la aplicación o no de esta normativa se suscitarán constantemente, es indispensable aplicar el principio de proporcionalidad que permita la vigencia de un régimen garantista de derechos y, al mismo tiempo, visibilizador de la actividad económica y tecnológica.

Consciente de que el RGPD establece el estándar de protección del derecho humano a la protección de datos personales, se ha estudiado su contenido con la finalidad de identificar aquellos elementos innovadores que marcan un progreso. En consecuencia,

> […] las reglas del RGPD contribuyen al establecimiento de un nuevo estándar global, que es exigible a los gobiernos de América Latina que contemplen ese estándar como la guía para la protección de sus propias ciudadanías. No es una cuestión de mera información o transparencia, sino de igualdad, libertad, autonomía y dignidad.[821]

[821] M. P. CANALES, J.C. LARA, "Lejos de proteger nuestros datos en américa latina", *@derechos digitales Derechos Humanos y Tecnologías en América Latina*, 3 de mayo de 2018, accedido el 15 de noviembre de 2019, https://www.derechosdigitales.org/12058/lejos-de-proteger-nuestros-datos-en-america-latina/

Adicionalmente, se ha realizado un estudio que consiste precisamente en identificar qué elementos se consideran sustanciales y, por ende, son inamovibles puesto que son parte de su esencia y garantizan la vigencia misma del contenido intrínseco del derecho. Este análisis permite la individualización del derecho, pues logra su diferenciación de otros. La identificación de los sutiles límites de su alcance y ámbitos, los niveles de aplicabilidad fáctica y las limitaciones admitidas que no afectan su naturaleza son los contornos que permiten definir el contenido esencial de la protección de las personas físicas en relación con el tratamiento de los datos de carácter personal.

Se puede concluir, entonces, que son parte del contenido esencial aquellos elementos que vienen desde la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre, relativa a la *protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*[822] y que fueron recogidos por la Ley de Protección de Datos de Carácter Personal 15/1999, de 13 de diciembre, de España, y de la vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[823], y que también son parte del vigente Reglamento General de Protección de Datos Personales. También se deber reconocer que las innovaciones introducidas por este último, igualmente deben ser consideradas como inherentes, debido a que han sido incorporadas para contrarrestar la realidad actual que plantea nuevas formas de transgresión; y porque todo avance en la protección de un derecho debe entenderse como incorporado a este debido a que la aplicación de los derechos humanos debe ser progresiva para garantizar su pleno reconocimiento y ejercicio.

Acorde al esquema de análisis que se utilizó como metodología, se puede establecer que el contenido del derecho a la protección de datos es el siguiente:

1. Elementos que constan desde las primeras normativas de protección de datos personales:

    a) *Ámbito de aplicación.* Delimitación del ámbito de aplicación del RGPD, que incluye la descripción del ámbito material, relativo a qué tipo de dato, su naturaleza, las condiciones propias de este, los tipos de soporte, entre otros, es aplicable del citado reglamento y del ámbito territorial, por el cual es aplicable el citado RGPD cuando un establecimiento trate datos personales, independientemente de si el tratamiento tiene lugar en la Unión o no. Así como, el tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión; o que tenga que aplicar la normativa europea en virtud del Derecho Internacional Público.

[822] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Diario Oficial n.° L 281, 23/11/1995, pp. 0031-0050, s. f.), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML.

[823] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, BOE.es, accedido 13 de noviembre de 2018, file:///C:/Users/Lorena/Desktop/Ley%20Protecci%C3%B3n%20datos%20y%20derechos%20digitales%20Espa%C3%B1a.pdf

b) *Naturaleza del dato.* Tratamiento de datos personales, incluidos aquellas categorías especiales de datos personales, independientemente del tipo de soporte en el que se encuentren y que puedan ser usados o no para hacer perfiles o estén seudoanonimizados.

c) *Sujeto activo.* Únicamente las personas físicas que a efectos del RGPD se denominan interesados.

d) *Sujeto pasivo.* El responsable del tratamiento, el encargado, el destinatario y el tercero, quienes deberán responsabilizarse por las violaciones o transgresiones reclamadas.

e) *Derecho de información.* El RGPD no lo menciona de forma expresa, sino que es parte del principio de transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado, puesto que determina la obligación de facilitar, por escrito o por otros medios, inclusive, si procede, por medios electrónicos, información al interesado relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada.

f) *Autodeterminación informativa.* En el RGPD no consta escrito en el texto, pero se vislumbra a todas luces de su contenido, ya que a través de todo el texto se materializan mecanismos de decisión, control y vigilancia sobre el tratamiento y uso de los datos personales por parte de sus titulares.

g) Necesidad de mandato legal para tratamiento sin autorización del titular. Ya no se trata de la legitimación sino de la licitud del tratamiento; es decir, cuando la ley determina es lícito y, por lo tanto, legítimo un tratamiento de datos personales.

h) Deber de información. El RGPD aborda el deber de información desde la perspectiva de obligaciones que el responsable de tratamiento debe cumplir respecto de los derechos del titular a ser informado y respecto de los riesgos, la finalidad, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos, cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento, las salvaguardas y los derechos y la forma de hacer valer estos derechos en relación con el tratamiento.

i) Principios de pertinencia, adecuación y minimización de datos. El principio de pertinencia se interrelaciona directamente con el de finalidad, ya que es indispensable saber para qué se usará un dato a fin de determinar su pertinencia; además, va de la mano del principio de adecuación y minimización de datos puesto que mediante estos se requerirá de medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inadecuados por inexactos o desactualizados, ajenos a los fines para los cuales fue recabado; y que se limite a un mínimo estricto el plazo de conservación del dato y su tratamiento se limite a la finalidad autorizada.

j) *Principio de calidad.* El RGPD, aunque no menciona de forma expresa el principio de calidad, si lo hace respecto de sus componentes: exactitud, veracidad y actualización de los datos personales. Estas características el responsable debe velar porque se cumplan en el momento de la recogida, pero fundamentalmente cuando son parte de las bases de datos de uso cotidiano, ya que si los datos no reflejan la realidad actual de una persona, puede significar la transgresión a sus derechos, incluso en el caso de nuevas finalidades y a múltiples cesiones o comunicaciones. Por eso, la mayor dificultad de este este principio es la actualización de los datos que posibilite su veracidad y exactitud, por lo que debe ir de la mano de los derechos de acceso, rectificación y cancelación.

k) *Principio de finalidad*. El RGPD establece que el principio de finalidad estipula que solo podrán ser recogidos, tratados y usados datos personales que hayan sido recogidos para fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. El responsable debe informar, especialmente, respecto de los fines específicos para garantizar un consentimiento inequívoco al titular y para permitir la vigilancia de la autoridad de control.

l) *Consentimiento explícito e inequívoco*. Está vetado el consentimiento tácito, por el que se presumía que ante la inacción del titular, su omisión significaba que consentía. Es posible el consentimiento implícito, que es el que se deduce de otra acción del interesado distinta del consentimiento.[824]

m) *Principio de tratamiento leal y transparencia de la información.* Presupone la prerrogativa que tiene toda persona de que el responsable y el encargado del tratamiento tomen medidas oportunas para facilitar al interesado toda información que debe ser puesta en su conocimiento en el momento de la recogida de datos y de la obtención del consentimiento; así como, la transparencia de las comunicaciones que se producen en el ejercicio de los derechos del titular para la presentación de reclamaciones; y las aplicables a toda información dirigida al público en general, que permita el ejercicio de los derechos subjetivos de las personas, de ser el caso y además el control ciudadano de estas actividades. Todo ello como una forma de reforzamiento de las relaciones de buena fe, lealtad y confianza en las distintas relaciones producto del tratamiento de datos personales. Tradicionalmente bastaba que la información se preste de modo expreso, preciso e inequívoco; ahora el RGPD requiere que la información respecto a las "condiciones de los tratamientos que afecten a titulares como en las respuestas a los ejercicios de derechos, deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo".[825]

n) *Principio de proporcionalidad.* El RGPD establece que el principio de proporcionalidad se aplica tanto en la interrelación del derecho a la protección de datos personales y otros derechos fundamentales, de tal forma que en caso de conflicto de derechos es indispensable realizar un ejercicio de ponderación, en el cual la proporcionalidad permita determinar los límites del derecho a la protección de los datos personales, sobre todo en su función social y de equilibrio con otros

[824] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, AGENCIA CATALANA DE PROTECCIÓN DE DATOS, Y AGENCIA VASCA DE PROTECCIÓN DE DATOS, *Guía del Reglamento General de Protección de Datos para responsables de tratamiento*.
[825] Ibíd.

derechos; como en el debate entre la protección de los datos de los titulares y el libre flujo informacional, es decir, entre el respeto por la dignidad humana y el desarrollo económico, social y cultural que los avances tecnológicos plantean; pero también es posible su aplicación en el momento de la imposición de sanciones.

o) *Principio de licitud.* El principio de licitud atañe a las condiciones legales establecidas expresamente en el RGPD que permiten el tratamiento de datos personales por parte de responsables y encargados, y que corresponde taxativamente a los siguientes: consentimiento, ejecución de un contrato, cumplimiento de una obligación legal, protección de intereses vitales, interés público o ejercicio de poderes públicos y satisfacción de intereses legítimos.

p) *Confidencialidad.* La confidencialidad aparece directamente relacionada con el derecho de seguridad, porque son complementarias, ya que constituye en los mecanismos adecuados, medidas técnicas, administrativas, organizativas y jurídicas que permiten la seguridad de la información y que tienen como consecuencia directa la confidencialidad de los datos personales. Inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

q) *Derecho de acceso.* El interesado tiene derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a información sobre: los fines del tratamiento, las categorías de datos personales de que se trate, los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, el plazo de conservación de los datos personales, la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento. Además, el derecho a presentar una reclamación ante una autoridad de control; cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen; la existencia de decisiones automatizadas, incluida la elaboración de perfiles, cuando se transfieran datos personales a un tercer país o a una organización internacional. También, acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales, copia de los datos personales objeto de tratamiento a través de medios electrónicos o de otros medios físicos.

r) Derecho de rectificación. Por el cual, se otorga al interesado el derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Asimismo, a que se completen los datos personales, tomando en cuenta los fines del tratamiento, inclusive mediante una declaración adicional.

s) Derecho de oposición. Por el cual, el interesado tiene derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento, incluida la elaboración de perfiles de personalidad.

t) Derecho de supresión. Por el cual, el interesado tiene derecho a que el responsable de tratamiento sin dilación indebida suprima los datos personales de su titularidad, cuando los datos personales ya no son necesarios para la finalidad para los que

fueron recogidos o tratados de otro modo; el interesado retire el consentimiento o se oponga al tratamiento; los datos personales hayan sido tratados ilícitamente; deban suprimirse para el cumplimiento de una obligación legal; si la retención de tales datos infringe el Reglamento, entre otras.

u) *Spam.* No existe en el RGPD mención alguna al *spam* o comunicaciones electrónicas no autorizadas.

2. Elementos que constituyen innovaciones introducidas por el RGPD:

a) *Principio de responsabilidad proactiva.* Por el cual, el responsable del tratamiento debe "tener una actitud consciente, diligente y proactiva frente a todos los tratamientos de datos personales que lleven a cabo"[826] y aplicar medidas técnicas y organizativas que permitan garantizar el cumplimiento de las obligaciones constantes en el RGPD; así como que pueda demostrarlo en el caso de ser requerido. Asimismo, realizar aquellas que aunque no estén escritas de forma específica, se deduzcan de la normativa como parte del deber mínimo de cuidado de los responsables y encargados de tratamiento.

b) *Seguridad adecuada al riesgo.* Por el cual se establece un sistema organizado, estratificado, estructurado e integral, que garantice un nivel de seguridad adecuado a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas propios del tratamiento, y aplicar medidas de prevención y mitigación, incluida la notificación de violaciones de seguridad.

c) *Derecho al olvido.* Por el cual, el titular solicita la eliminación de los datos personales que un responsable haya hecho públicos, incluido todo enlace a ellos, o las copias o réplicas de tales datos cuando esta información transgreda los principios de finalidad, licitud, lealtad, transparencia, consentimiento, entre otros. Para lo cual, el responsable del tratamiento deberá tomar en cuenta la tecnología disponible y el coste de su aplicación, y adoptar medidas razonables, incluidas medidas técnicas.

d) *Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales.* Todo interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos o le afecte significativamente de modo similar.

e) *Derecho de consulta al registro general de protección de datos personales*. No consta en el RGPD el derecho de consulta al registro general de protección de datos por parte del interesado, sino únicamente la obligación del responsable, del encargado o de sus representantes, de realizar un registro de bases de datos efectuadas bajo su responsabilidad, para ponerlo a disposición de la autoridad de control que lo solicite, a efectos de facilitarle su labores de control.

[826] *Ibíd.*

f) *Derecho a indemnización por daños causados.* Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de un tratamiento en infracción del Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

g) *Derecho a limitar el tratamiento*. Por el cual, el interesado tiene derecho a obtener del responsable la limitación del tratamiento de los datos personales, cuando se va a solicitar su eliminación, o se ha impugnado su exactitud, ilicitud, su necesidad de conservación o por motivos legítimos, mientras se verifica si los motivos del responsable son legítimos y prevalecen sobre los del interesado.

h) *Derecho a la portabilidad.* El interesado tiene derecho a recibir los datos personales que haya facilitado a un responsable del tratamiento y a transmitirlos a otro directamente, sin que lo impida el responsable al que se los hubiera facilitado, cuando sea técnicamente posible. Además, a recibir estos datos en un formato estructurado, de uso común, para lectura mecánica y con formatos interoperables que permitan la portabilidad de datos.

i) *Restricciones a las obligaciones, los derechos y los principios.* El RGPD establece, mediante medidas legislativas, limitaciones aplicables al alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 (acceso, rectificación, supresión, derecho al olvido, oposición, portabilidad, limitación al tratamiento, no soportar decisiones individuales automatizadas, incluida la elaboración de perfiles), así como las contenidas en el artículo 34 relativas a las notificaciones de las violaciones de seguridad y las del artículo 5 respecto a los principios en su relación con los citados derechos y obligaciones; incluso en aquellas conexas cuando primen necesidades asociadas al bien común y al interés general en cuanto al derecho a la protección de datos personales individuales. Esta figura permite establecer el contenido esencial mínimo; es decir, aquellos elementos indispensables que no pueden ser disminuidos y que están relacionados con: la naturaleza del dato, el objeto o bien jurídico en el que consta el derecho información, la autodeterminación informativa y la necesidad de mandato legal, así como los principios de finalidad, de licitud, de conservación, determinación de los sujetos activos y pasivos, y los derechos.

j) *Obligaciones generales.* Que describe aquellas obligaciones en el tratamiento del responsable o del encargado, de los representantes de responsables o encargados del tratamiento, incluidas las corresponsabilidades, las formalidades en la elección de otros encargados, el contenido mínimo del contrato del encargado, las cláusulas contractuales tipo, el delegado de protección de datos personales, la protección de datos desde el diseño y por defecto, los códigos de conducta, las certificación de en materia de protección de datos y de sellos y marcas de protección de datos, la evaluación de impacto relativa a la protección de datos y la consulta previa. Varias de estas obligaciones, además de ser una novedad, representan un cambio de configuración en la posición proactiva y diligente de quienes traten datos personales.

k) *Procedimientos. El régimen* que garantice el ejercicio de derechos de los titulares mediante mecanismos para solicitar acceso, rectificación, supresión u oposición directamente al responsable o encargado del tratamiento como: el derecho a presentar una reclamación ante una autoridad de control única; el derecho

a la tutela judicial efectiva contra una autoridad de control; el derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento; derecho a indemnización y responsabilidad.

l) *Institucionalidad de protección.* Que determina la existencia de una o varias autoridades de control, del Comité Europeo de Protección de Datos y de la Comisión como un sistema jerarquizado, orgánico y armónico que permita viabilice el seguimiento, la supervigilancia y el control de la aplicación del RGPD con absoluta independencia. En el cual las funciones de cada uno estén adecuadamente definidas, así como sus poderes públicos sean claros y efectivos, los mecanismos de cooperación y coherencia entre autoridades, de asistencia mutua y operaciones conjuntas permitan una aplicación uniforme de las decisiones, asimismo la inmediatez en los procedimientos de urgencia.

m) *Régimen sancionador.* Por el cual, se postulan sanciones administrativas mediante poderes correctivos, además de multas administrativas que en conjunto de forma simultánea o no se aplican a las infracciones suscitadas por responsables y encargados, y que por su fuerza coercitiva motivan, como sistema de prevención general, el cumplimiento de las disposiciones del RGPD a título de que su transgresión resulta gravosa para quien incurra en ella.

n) *Transferencia internacional de datos.* Se considera como principio general de las transferencias, el cumplimiento de una serie de condiciones que aseguren el intercambio transfronterizo de datos con terceros países u organismos internacionales que tengan un nivel adecuado de protección sobre la base de varios mecanismos como: una decisión de adecuación dictada por la Comisión, mediante un acto de ejecución; de garantías adecuadas entregadas por el responsable o por una autoridad de control; de normas corporativas vinculantes; o mediante excepciones para situaciones específicas descritas en el RGPD, y en casos aislados la transferencia de datos a terceros países a los que no les ampara ningún mecanismo transfronterizo de datos a terceros países con apego irrestricto a ciertas condiciones descritas en el reglamento. Este régimen de protección, se establece como un modelo que ante la dificultad sobre todo técnica de cobijar los datos de personas que constantemente salen del territorio europeo, lo que dificulta el control, intenta universalizar el estándar europeo como hegemónico en el mundo, desde la perspectiva de que es el que da mayores garantías para el ser humano, como centro de todo desarrollo tecnológico, social, económico y cultural.

De lo transcrito se establece que mientras más avances científicos y técnicos se desarrollen, respecto del tratamiento de datos personales, se irán ampliando los requisitos, características condiciones y presupuestos que permitan garantizar la protección de la persona física. Esta realidad evidencia que el derecho tiene el mayor reto de todos, y debe ir un paso adelante o al menos a la par, para evitar transgresiones a los derechos de las personas, pues en la medida en que se comprenden las repercusiones de estas realidades, más vulneraciones se encuentran, no solo al individuo sino incluso a la democracia, a la libertad de expresión, a las bases mismas de la organización de un Estado de derecho.

CAPITULO III

ARMONIZACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES EN AMÉRICA LATINA A TRAVÉS DE INSTRUMENTOS INTERNACIONALES

Con la finalidad de aprovechar el potencial de las TIC para el desarrollo sostenible, generar confianza en línea y garantizar las oportunidades que brindan los adelantos tecnológicos, cada uno de los países, sobre la base de su estructura normativa propia, ha optado por desarrollar mecanismos de protección de las personas y sus datos.

Hay pocos Estados que no han desarrollado normativa alguna sobre la materia, o la que tienen es incompleta, dispersa o contradictoria; estos son los que mayor desventaja presentan no solo frente a los riesgos y peligros que trae consigo el manejo de datos personales, sino ante la imposibilidad de usarlos como insumos clave para su desarrollo económico y social, lo cual evidencia la posibilidad real de quedar aún más rezagados.

Es indispensable dar certidumbre a usuarios, empresas, organizaciones y Estados, sobre todo en este momento en el cual la economía mundial se desplaza hacia un espacio de información masiva; hiperconectada; en tiempo real; de flujo incesante proveniente del internet de las cosas; automatizada con algoritmos de inteligencia artificial cada vez más sofisticados; y, de la réplica incesante mediante tecnologías de registros distribuidos. Todo esto, unido a que, los datos no tienen fronteras, además plataformas y servicios son de libre disposición y almacenan información en centros virtuales en todo el mundo. Todo lo cual, obliga a los países a realizar marcos jurídicos compatibles en distintos niveles: nacional, regional y mundial, que faciliten el intercambio y al mismo tiempo respete y proteja derechos humanos.

En este contexto, varias naciones, sobre todo aquellas que pertenecen al *common law*, abordan el tema de los datos personales a través *the right to privacy*. El derecho de las personas a mantener fuera del conocimiento público aquellos aspectos de la vida que se consideran de orden privado, personal, familiar o social y que no debe ser puesto en conocimiento de otros, sin justa causa o autorización del titular. De modo que, son los titulares los que deciden qué aspectos de su vida desean o no compartir y para qué finalidad.

En Estados Unidos, la *privacy* sube a rango constitucional como manifestación de la Cuarta Enmienda, que hace referencia a la prohibición de pesquisas y aprehensiones arbitrarias. Actualmente, se interpreta como la norma que protege, lo privado de cada persona, incluida la correspondencia, efectos o enseres, de la intromisión ilegal de un tercero; por eso la necesidad de sentencia judicial para su efectivo ejercicio. Es un modelo de protección asociado a la propiedad privada, desde el derecho a ser dejado en paz, a estar solo[827].

[827] A. M. BENDICH, Privacy, *Poverty and the Constitution, Conference on the Law of the por*, accedido el 3 de noviembre de 2019, https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2925&context=californialawreview

Debido a las graves afectaciones a las libertades individuales producidas por Cambridge Analitics y Facebook[828], el modelo de *privacy* está en crisis[829]. Esto porque la visión inicial que exigía por parte del Estado o de particulares, únicamente, un deber de abstención, de evitar molestar o transgredir al otro, resulta limitada. En primer lugar, porque el titular del derecho solo podía exigir su cumplimiento cuando este había sido violentado. En segundo lugar, porque el nivel de exposición de los datos no es el único factor de riesgo sino los usos inadecuados que se pueda dar incluso a datos personales que el propio usuario dispone como de acceso general. Pero sobre todo, el caso citado, deja en evidencia que el uso inadecuado de los datos personales no solo transgrede la *privacy* sino otros derechos fundamentales como la libertad de pensamiento, de opinión, de conciencia y de voto.

Entonces, es contradictorio, que se necesite de la existencia de un daño para que un titular pueda reclamar, cuando es posible arbitrar medidas que permitan evitar que este se produzca. Adicionalmente, se depositaba en el otro el deber pasivo negativo de no hacer nada para que sobre la base de la inacción se pueda asegurar la vigencia de un derecho.

En consecuencia, la realidad social ha visto la necesidad de ir adaptando la normativa para ir estableciendo verdaderos marcos de protección. De esta forma, estamos mirando

---

[828] Este proceso empezó cuando en la Universidad de Cambridge un psicólogo ruso desarrolló una aplicación que permitía acceder a la información de todos los usuarios de diversas redes sociales, con fines académicos e investigativos. Tan solo se había conseguido el consentimiento de 270.000 personas; no obstante, la *app* accedía a los datos de 50 millones de personas conectadas a Facebook. Los datos fueron compartidos con la empresa Cambridge Analityca, lo cual significó que los datos de más de un tercio de sujetos estadounidenses activos, que representaban la cuarta parte de votantes potenciales de este país, estaba almacenada en una base de datos perteneciente a la mencionada compañía. T. BERNERS-LEE, "El escándalo de Facebook y la filtración de datos para usos políticos".
Cambridge Analityca es una empresa orientada a administrar campañas políticas en medios digitales; se caracteriza por enviar mensajes masivos, dirigidos y especializados a personas de acuerdo con sus preferencias, ideología política y pasiones. Casualmente, el jefe de campaña de Donald Trump fue socio de esta compañía, la cual fue contratada para subir la simpatía por el candidato y pudiera ganar las elecciones presidenciales. "The Observer view on how Facebook's destructive ethos imperils democracy | Observer editorial | Opinion | The Guardian", accedido 18 octubre 2018, https://www.theguardian.com/commentisfree/2018/mar/17/observer-view-facebook-harvesting-data-cambridge-analytica-files.
De ese modo, con la finalidad de influir en la decisión de los votantes estadounidenses, Cambridge Analityca formó audiencias a las cuales se envió anuncios publicitarios con contenido diferenciado para republicanos y demócratas. Además, se logró establecer a qué ciudades debía viajar el candidato para ganar simpatía; todo esto con la información que fue obtenida de la aplicación que permitía el acceso a los datos de Facebook, en donde se monitoreaba los *likes* que cada usuario daba. "Mark Zuckerberg - The New York Times", accedido 17 octubre 2018, https://www.nytimes.com/topic/person/mark-zuckerberg.
El 17 de marzo de 2018 las portadas del *The New York Times (*"How Trump Consultants Exploited the Facebook Data of Millions - The New York Times", accedido 18 octubre 2018, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html)
y *The Observer / The Guardian*) habían develado toda la información que llevaría a Mark Zuckerberg a dar declaraciones ante el Senado estadounidense y el Parlamento Europeo, ante la cesión de datos a Cambridge Analityca para influir en la campaña política de Donald Trump, y a través de noticias falsas incidir en las elecciones y posiblemente contribuir en su triunfo electoral.

[829] "El escándalo de Cambridge Analytica muestra cuánto daño pueden hacer las tecnologías a la privacidad cuando su diseño se centra únicamente en los beneficios o la usabilidad". RED INTERNACIONAL DE ORGANIZACIONES DE LIBERTADES CIVILES, *El derecho a la privacidad en la era digital*, abril de 2018, acccedido el 3 de noviembre de 2019, file:///C:/Users/Lorena/Desktop/Informaci%C3%B3n%20tesis/relator%C3%ADas/nuevos/revisados/INCLO-OHCHR.pdf

iniciativas como la *California Consumer Privacy Act Bill Text - AB-375 Privacy: personal information: businesses*[830] que incluyen en la *privacy* elementos o contenidos propios del modelo europeo[831].

De otro lado, el enfoque de protección europeo, que pertenece al *civil law*, reconoce como derecho autónomo e independiente a la protección de datos personales. De tal manera que, no se protege únicamente ámbitos o esferas asociadas a la intimidad personal, familiar o social sino que se busca una protección integral del individuo, quien no puede estar protegido por partes sino que lo debe estar en todas sus manifestaciones en el entorno digital.

Como se analizó oportunamente, en el segundo capítulo de este trabajo, el sistema de protección continental, inicio desde la asociación del derecho a la intimidad al entorno digital. Esta postura fue ampliamente superada porque para garantizar una protección completa del individuo no se lo puede segmentar. No es posible diferenciar, en el mundo virtual, qué datos personales son íntimos, privados o de conocimiento común, ya que incluso sus fragmentos o aquellos considerados inocuos o superficiales, agrupados entre sí, a través de tecnologías como el *dataminig* o el *big data*, entre otras, pueden otorgar perfiles completos de los individuos. Todo lo cual, generó el nacimiento de un derecho autónomo e independiente denominado derecho a la protección de datos personales.

En el caso de los países latinoamericanos, la mayoría de ellos pertenecen al modelo del *civil law* y en tal virtud, han adoptado el modelo europeo más garantista de derechos; en tal sentido, la mayoría de las normativas constitucionales de la región han incorporado al *habeas data*. Esta figura jurídica tiene una doble dimensión, ser garantía o mecanismo procesal constitucional y al mismo tiempo derecho fundamental. Sobre sus

[830] "California Consumer Privacy Act Bill Text - AB-375 Privacy: personal information: businesses", 2018, accedido 17 octubre 2019, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=California+Consumer+Privacy+Act+of+2018.

[831] Los derechos que comprende la *California Consumer Privacy Act Bill Text - AB-375 Privacy, personal information, businesses* y que se asimilan al modelo europeo son los siguientes:

1. Derecho a conocer todos los datos que constan en las empresas, al menos dos veces al año y que el acceso a esta información no tenga ningún costo.
2. Derecho a expresar el deseo de que NO se venda la información propia de cada persona.
3. Derecho a la seguridad de la información; es decir, derecho a demandar en caso de que las empresas que se encontraban a cargo de los datos personales de cada persona, no hayan sido diligentes y como consecuencia de ello esa información se haya perdido o haya sido robada.
4. Derecho a eliminar la información que anteriormente ha sido cargada en cualquier base de datos.
5. En caso de que el titular de la información haya expresado su deseo de que sus datos no sean vendidos, por ninguna circunstancia podrá ser discriminado, y recibirá el mismo trato que los demás consumidores.
6. Toda persona tendrá derecho a que se le informe sobre las diversas categorías de datos que recopila cada empresa; así también, el manejo que se les dé a los mismos.
7. En el caso de la información de menores de 16 años, de forma obligatoria se debe expresar el consentimiento o rechazo a la venta de su información.
8. Derecho a conocer las categorías de terceros con los que se comparten sus datos.
9. Derecho a conocer las categorías de fuentes de información de las que se adquirieron sus datos.
10. Derecho a conocer la finalidad comercial o comercial con que se recopila su información.

Cabe recalcar que todos los procesos que se deriven de la implementación de la norma serán resueltos por medio de una acción privada solo en los casos de violaciones de datos; todos los demás procesos se darán a conocer al Procurador General de California, y como sanción se podrán establecer multas de hasta US $ 2.500 dólares por cada violación que se haya cometido.

características y contenidos en la región se analizará en el capítulo cuarto de este trabajo. Así mismo, varios países latinoamericanos de forma independiente o simultáneamente han reconocido el derecho a la protección de datos personales en sus Cartas Magnas o a través de normativa legal especializada.

Como vemos, cada país, debido a los sistemas jurídicos a los que pertenecen y a condiciones propias de su desarrollo económico, político y social han definido la dimensión y alcance de la protección de los datos personales ya sea a través de la *privacy* o del reconocimiento de este derecho autónomo.

Ahora bien, a continuación se revisará varios instrumentos internacionales que tienen influencia directa en la región, debido a que, provienen de entidades creadas por convenios o tratados internacionales ratificados por países Latinoamericanos. Estos instrumentos de manera general son: informes anuales de la Relatoría Especial para la Libertad de Expresión de la Organización de Estados Americanos, así como las posturas del nuevo Relator Especial de la Privacidad; varias resoluciones de la Corte Interamericana de Derechos Humanos que pueden ser aplicables; así como aquellas Recomendaciones de la OEA relacionadas con la temática; las Directrices y Resoluciones de Naciones Unidas sobre el derecho de privacidad en la era digital y otros similares. Finamente, los Estándares de protección de datos personales para países iberoamericanos elaborado por la Red Iberoamericana de Protección de datos personales con el que se intenta armonizar las legislaciones locales, hasta que se pueda construir normativa comunitaria que permita un libre flujo informacional que habilite un ecosistema digital sano, confiable y eficiente.

1. Antecedentes internacionales del derecho a la protección de datos en Latinoamérica

Los primeros antecedentes internacionales del derecho a la protección de datos en Latinoamérica se remontan a la Declaración Universal de los Derechos Humanos; adoptada por la Asamblea General mediante la Res. 217 A (III), de 10 de diciembre del 1948, señala: "Artículo 12.- Toda persona debe ser protegida ante injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, así como de ataques contra su honra y reputación". Asimismo, en la Declaración Americana de los Derechos y Deberes del Hombre, aprobada en la Novena Conferencia Internacional Americana realizada en Bogotá en el año 1948, consta lo siguiente: "Artículo V. Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar".

Estas normativas coinciden en determinar la existencia de un derecho fundamental creado para proteger a los individuos de injerencias o ataques a su ámbito personal y familiar.

Texto muy similar consta descrito en el artículo 8 del Convenio Europeo de los Derechos Humanos y de las Libertades Fundamentales, celebrado en Roma, el 4 de noviembre de 1950. Aquí, la diferencia radica en el numeral dos, el cual establece casos excepcionales de autorización, es decir que solo podrá justificarse una intromisión o injerencia a la vida privada o familiar cuando esté autorizada por ley y por "razones de

seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de los derechos y las libertades de los demás".

Asimismo, el artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos de Naciones Unidas, aprobado por la Res. 2.200 A (XXI) de la Asamblea General de 16 de diciembre de 1966, que entró en vigor el 23 de marzo de 1976, además de proscribir los ataques contra la vida privada y la familia añade otros espacios de resguardo, estos son el domicilio y la correspondencia, conforme consta del texto que se transcribe a continuación:

> Artículo 17. 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. | 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Posteriormente, la Convención Americana de Derechos Humanos de 1969, celebrada en San José, Costa Rica del 7 al 22 de noviembre de dicho año, nuevamente recoge el deber de respeto del espacio privado de las personas:

> Artículo 11. Protección de la Honra y de la Dignidad.- 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. | 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. | 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

De los contenidos casi idénticos de las citadas normas, se puede colegir que se configura un deber de abstención o dimensión negativa[832] que impide al Estado y a los particulares realizar cualquier tipo de injerencia arbitraria, abusiva o ilegal que afecte en términos generales la dignidad humana. Así, se entendería que para realizar una acción que la perturbe sería necesaria una adecuada ponderación de derechos y la existencia de una disposición legal que la faculte.

Además, mediante este deber de abstención se protegen varios derechos humanos como son los expresamente señalados: honra o reputación; así como, aquellos que pueden ser identificados de la simple extracción de los contenidos esenciales descritos en las citadas normas como son: intimidad, privacidad, inviolabilidad de domicilio, inviolabilidad de correspondencia y libre desarrollo de la personalidad. Derechos que han sido incorporados en las Constituciones latinoamericanas con diferentes formas de redacción, que evidencian también las distintas comprensiones que cada país ha tenido de ellos.

Ahora bien, las primeras luces sobre la necesidad de proteger a las personas del abuso en el uso de la tecnología llegan a América mediante instrumentos internacionales que empezaban a tratar de estos temas.

El Pacto Internacional de Derechos Económicos, Sociales y Culturales fue aprobado por la Res. 2200 A (XXI) de la Asamblea General de 16 de diciembre de 1966, y entró en vigor el 3 de enero de 1976; respecto de los adelantos científicos señala:

---

[832] I. BERLÍN, *Cuatro ensayos sobre la libertad* (Madrid: Alianza, 1998), 229.

> Artículo 15 1. Los Estados Partes en el presente Pacto reconocen el derecho de toda persona a: a) Participar en la vida cultural; b) Gozar de los beneficios del progreso científico y de sus aplicaciones...

A su vez, la Conferencia Internacional de Derechos Humanos, celebrada en Teherán el 13 de mayo de 1968, que se convocó para "examinar los progresos logrados en los veinte años transcurridos desde la aprobación de la Declaración Universal de Derechos Humanos y preparar un programa para el futuro" y en la que los Estados participantes señalaron que:

> 18. Si bien los recientes descubrimientos científicos y adelantos tecnológicos han abierto amplias perspectivas para el progreso económico, social y cultural, esta evolución puede, sin embargo, comprometer los derechos y las libertades de los individuos y por ello requerirá una atención permanente...

Como se vio en el capítulo que corresponde al sistema de protección europeo las primeras resoluciones y normativa que reconoce la vulnerabilidad de la privacidad familiar y personal por el uso de la informática y la tecnología, y que plantea proteger los derechos de las personas en estos nuevos ámbitos de su desarrollo social, se remontan a Alemania mediante la sentencia del Censo (1970).[833] Posteriormente, la primera norma que hace mención específica a la protección de los datos personales es de origen suizo, denominada Data Act (1973).

La respuesta latinoamericana a esta tendencia de proteger a las personas de las transgresiones producidas por la tecnología y la informática, en lo relativo a datos personales, aparecieron por primera vez en la Constitución de Guatemala de 1985[834] mediante la normativa que intentaba proteger los datos de las personas respecto de abusivas injerencias por parte de los Estados. Posteriormente, emergió por vez primera en Brasil en 1988[835] una figura propia denominada *habeas data*, concebida como garantía constitucional. Ahora bien, cada país latinoamericano fue incorporando, desde sus propias perspectivas, formas de protección de los datos personales, las cuales serán analizadas en el siguiente capítulo de este trabajo.

Consecutivamente, la Conferencia Mundial de Derechos Humanos celebrada en Viena del 14 a 25 de junio de 1993 aprueba la Declaración y el Programa de Acción de Viena, la cual al referirse a la informática señala:

> 11. El derecho al desarrollo debe realizarse de manera que satisfaga equitativamente las necesidades en materia de desarrollo y medio ambiente de las generaciones actuales y futuras. [...] Todos tienen derecho a disfrutar del progreso científico y de sus aplicaciones. La Conferencia Mundial de Derechos Humanos toma nota de que ciertos adelantos, especialmente en la esfera de las ciencias biomédicas y biológicas, así como en la esfera de la informática, pueden tener consecuencias adversas para la integridad, la dignidad y los derechos humanos del individuo y pide la cooperación internacional para

[833] R. HUBER, ed., *Jurisprudencia del Tribunal Constitucional Federal Alemán, Extractos de las sentencias más relevantes compiladas por Jürgen Schwabe*, Konrad - Adenauer - Stiftung e. V, México, DF. 2009, 99, accedido 20 de noviembre de 2017, http://www.kas.de/wf/doc/kas_16817-544-4-30.pdf.
[834] Guatemala, *Constitución Política de la República de Guatemala* [1985], reformada en 1993.
[835] Brasil, *Constitución de la República Federativa del Brasil* [1988].

> velar por el pleno respeto de los derechos humanos y la dignidad de la persona en esta esfera de interés universal.

De lo visto se desprende que aquellos derechos consagrados por la Declaración Universal de Derechos Humanos, por el Pacto Internacional de los Derechos Civiles y políticos de Naciones Unidas y por la Convención Americana de Derechos Humanos deben ser comprendidos desde nuevas perspectivas: científica, tecnológica e informática. Los avances que constantemente se producen en estas áreas pueden llegar a afectar la dignidad y los derechos humanos, y en tal sentido, debe propenderse a una protección integral de las personas que incluya estas esferas.

En esos instrumentos se visibiliza la preocupación de los países, inicialmente en 1968, por las posibles repercusiones negativas de los avances científicos y adelantos tecnológicos especialmente en el campo de las libertades individuales, para posteriormente, en 1993, reconocer a la esfera de la informática como uno de aquellos avances que si bien permiten el progreso científico pueden afectar además de la libertad, la dignidad y, en general, los derechos humanos de un individuo. Así, se insta a las naciones a velar por el respeto de los derechos y dignidad de la persona, reconociendo a la misma en su relación con la informática como una esfera de interés universal.

Por eso, en orden cronológico resta analizar los otros documentos internacionales que hacen mención a las transgresiones de la informática y la tecnología, a los derechos humanos, en especial a la intimidad y al derecho a la protección de datos personales.

El Consejo de Europa dictó el Convenio Nº108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, adoptado en Estrasburgo, y el Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos adoptado en Estrasburgo, el 8 de noviembre de 2001. Anotándose que, este el primer instrumento internacional que reconoce el derecho a la protección de los datos de las personas y actualmente ha sido ratificado por Uruguay (2012), México (2018) y Argentina (2019).

Asimismo, en la Declaración de Principios sobre Libertad de Expresión elaborado por la Relatoría para la Libertad de Expresión[836], reconoce el derecho de todas las personas de acceder a información sobre sí misma o sus bienes.

Para el 15 noviembre de 2003 se produjo la Declaración de Santa Cruz de la Sierra[837], por la cual los Jefes de Estado y de Gobierno de veintiún países iberoamericanos manifestaron, en su numeral 45 que:

---

[836] "La Relatoría Especial fue creada por la CIDH en octubre de 1997, durante su 97º Período de Sesiones, por decisión unánime de sus miembros. La Relatoría Especial fue establecida como una oficina permanente e independiente que actúa dentro del marco y con el apoyo de la CIDH. Con ello, la CIDH buscó estimular la defensa hemisférica del derecho a la libertad de pensamiento y de expresión, considerando su papel fundamental en la consolidación y desarrollo del sistema democrático, así como en la protección, garantía y promoción de los demás derechos humanos". OEA - Organización de los Estados Americanos: "Democracia para la paz, la seguridad y el desarrollo", 2009, accedido 1 de mayo de 2017, http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=132&lID=2.

[837] XIII Cumbre Iberoamericana de Jefes de Estado y Gobierno, *Declaración de Santa Cruz de la Sierra*, 2003, accedido 2 de mayo de 2017, http://segib.org/wp-content/uploads/DeclaraciondeSantaCruz.pdf

> […] la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenida en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad. [838]

Asimismo, en el II Encuentro iberoamericano de protección de datos, los participantes suscriben la Declaración de la Antigua Guatemala – II EIPD 2003[839], en el cual además de reiterar a la protección de datos personales como un derecho fundamental, se cristaliza la Red Iberoamericana de Protección de Datos Personales, al establecer la forma de su integración y su funcionamiento, tal como señalan el siguiente texto:

> 1º Valoran el creciente interés, preocupación y compromiso que en el ámbito de los Países Iberoamericanos se ha puesto de manifiesto con la protección de datos personales. 2º Reiteran la consideración de la protección de datos personales como un auténtico derecho fundamental de las personas, sobre todo en orden al respeto a su intimidad y de su facultad de control y disposición sobre los mismos. 5º Constatan la necesidad de impulsar la adopción de medidas que garanticen un elevado nivel de protección de datos, así como la idoneidad de contar con marcos normativos nacionales que, inspirados en tradiciones jurídicas comunes, en el respeto a los derechos fundamentales y en los intereses de sus respectivos países, garanticen una protección adecuada en todos los Países Iberoamericanos. Tales marcos normativos deberían tomar en consideración los principios esenciales de protección de datos reconocidos en los instrumentos nacionales. En este sentido, consideran muy positivas las iniciativas regulatorias que se han puesto en marcha en diversos Países Iberoamericanos. 6º Resaltan la importancia de potenciar las iniciativas de intercambio de experiencias entre los Países Iberoamericanos, estableciendo canales permanentes de diálogo y colaboración en materia de protección de datos. 7º Con este fin, y al objeto de reforzar la mutua y continua colaboración entre ellos, avanzando en base al Foro Permanente creado con ocasión del Primer Encuentro, se constituyen en la Red Iberoamericana de Protección de Datos, abierta a la incorporación de representantes de todos los Países Iberoamericanos.[840]

En el III Encuentro Iberoamericano de protección de datos, se suscribe la Declaración de Cartagena de Indias, III EIPD 2004[841], en la que se concientiza sobre el rol informativo de la Red Iberoamericana de Protección de Datos para la comprensión de la aplicación e impacto de la protección de datos en cada país de la región, de tal forma que los participantes deciden asumir una actitud más proactiva, en procura de logros más concretos. Se han realizado un total de XV encuentros hasta el año 2017[842], en cada uno de ellos, se culmina con la firma de una Declaración. Estas no tienen efectos vinculantes pero son marcos referenciales de buenas intenciones, mecanismos de

[838] Ibíd.
[839] II Encuentro iberoamericano de protección de datos, *Declaración de La Antigua – Guatemala, 2003*, accedido 5 de septiembre de 2019, http://www.redipd.es/documentacion/common/declaracion_2003_II_encuentro_es.pdf
[840] Ibíd.
[841] III Encuentro Iberoamericano de protección de datos, *Declaración de Cartagena de Indias, III EIPD,* 2004, accedido 05 de septiembre de 2019, http://www.redipd.es/documentacion/common/declaracion_2004_III_encuentro_es.pdf
[842] Red Iberoamericana de Protección de Datos Personales, *Documentos Generales: Declaraciones RIPD,* accedido 05 de septiembre de 2019, http://www.redipd.es/documentacion/index-ides-idphp.php

coordinación, espacios de diálogo y de planificación para el trabajo en conjunto de los interesados en armonizar la protección en la zona.

Hito esencial en el avance de la universalización del reconocimiento de la protección de datos como derecho fundamental consta en la Cumbre Mundial sobre la Sociedad de la Información (CMSI) que se desarrolló en dos fases. La primera, por medio de la Cumbre Mundial de la Sociedad de la Información realizada en Ginebra entre el 10 al 12 de diciembre de 2003, y la segunda, mediante la Cumbre Mundial de la Sociedad de la Información celebrada en Túnez, del 16 al 18 de noviembre de 2005.

Estas Cumbres constituyen un hito, no solo para las Naciones Unidas y la Unión Internacional de Telecomunicaciones, pues abordan energéticamente "cuestiones planteadas por las tecnologías de la información y la comunicación (TIC) a través de un enfoque estructurador e integrador".[843]

Cabe hacer referencia a la Declaración de Principios de Ginebra de 2003[844], específicamente al apartado B que se refiere a una Sociedad de la Información para todos: principios fundamentales:

a) Apartado B5 relativo al *fomento de la confianza y seguridad en la utilización de las TIC*, numeral 35 consta lo siguiente:

> B5. 35. El fomento de un clima de confianza, incluso en la seguridad de la información y la seguridad de las redes, la autenticación, la privacidad y la protección de los consumidores, es requisito previo para que se desarrolle la Sociedad de la Información y para promover la confianza entre los usuarios de las TIC. Se debe fomentar, desarrollar y poner en práctica una cultura global de ciberseguridad, en cooperación con todas las partes interesadas y los organismos internacionales especializados. Se deberían respaldar dichos esfuerzos con una mayor cooperación internacional. Dentro de esta cultura global de ciberseguridad, es importante mejorar la seguridad y garantizar la protección de los datos y la privacidad, al mismo tiempo que se amplía el acceso y el comercio. Por otra parte, es necesario tener en cuenta el nivel de desarrollo social y económico de cada país, y respetar los aspectos de la Sociedad de la Información orientados al desarrollo. [845]

b) Apartado B10 respecto a las *dimensiones éticas de la sociedad de la información*, numeral 58, aparece lo que sigue:

> B10.58. El uso de las TIC y la creación de contenidos debería respetar los derechos humanos y las libertades fundamentales de otros, lo que incluye la privacidad personal y el derecho a la libertad de opinión, conciencia y religión de conformidad con los instrumentos internacionales relevantes.[846]

[843] Ginebra, Unión Internacional de Telecomunicaciones; Naciones Unidas, *Documentos finales de la Cumbre Mundial de la Sociedad de la Información*, 2005, accedido 1 de mayo de 2017, https://www.itu.int/net/wsis/outcome/booklet-es.pdf.
[844] Cumbre Mundial sobre la sociedad de la información, *CMSI: Declaración de Principios de Ginebra*, 2003, accedido 2 de mayo de 2017, http://www.itu.int/net/wsis/docs/geneva/official/dop-es.html.
[845] Ibíd.
[846] Ibíd.

Entretanto, en el Plan de Acción de Ginebra de 2003[847] constan varios elementos relativos a la privacidad y al derecho a la protección de datos personales que luego serían parte, tanto del Compromiso de Ginebra como del de Túnez.

a) Apartado B5, relativo a la creación de confianza y seguridad en la utilización de las TIC, en el numeral 12, literales c) y f), consta lo siguiente:

> B5. 12. La confianza y la seguridad son unos de los pilares más importantes de la Sociedad de la Información: [...] c) Los gobiernos y otras partes interesadas deben fomentar activamente la educación y la sensibilización de los usuarios sobre la privacidad en línea y los medios de protección de la privacidad [...] f) Seguir fortaleciendo el marco de confianza y seguridad con iniciativas complementarias y de apoyo mutuo en los ámbitos de la seguridad en el uso de las TIC, con iniciativas o directrices sobre el derecho a la privacidad y la protección de los datos y de los consumidores. [848]

b) Apartado C6, sobre el entorno habilitador, en el numeral 13, literal i) se señala lo siguiente:

> C6. 13. i) Los gobiernos y las partes interesadas deben promover activamente la educación y la sensibilización de los usuarios en cuanto a la privacidad en línea y los medios para proteger la privacidad. [849]

c) Apartado C7, sobre aplicaciones de las TIC: ventajas en todos los aspectos de la vida, en su numeral 18, respecto de Cibersalud, manifiesta los siguientes literales a) y d):

> C7. 18. a) Promover la colaboración entre gobiernos, planificadores, profesionales de la salud y otras entidades, con la participación de organizaciones internacionales, para crear sistemas de información y de atención de salud fiables, oportunos, de gran calidad y asequibles, y para promover la capacitación, la enseñanza y la investigación continuas en medicina mediante la utilización de las TIC, respetando y protegiendo siempre el derecho de los ciudadanos a la privacidad [...] d) Promover el desarrollo de normas internacionales para el intercambio de datos sobre salud, teniendo debidamente en cuenta las consideraciones de privacidad. [850]

d) Apartado C10, relativo a las dimensiones éticas de la Sociedad de la Información, en cuyo numeral 25, literal c), consta el siguiente pasaje:

> C10. 25. c) Todos los actores de la Sociedad de la Información deben promover el bien común, proteger la privacidad y los datos personales así como adoptar las medidas preventivas y acciones adecuadas (según lo establecido en la ley), contra la utilización abusiva de las TIC, tales como las conductas ilegales y otros actos motivados por el racismo, la discriminación racial, la xenofobia y las formas conexas de intolerancia, el odio, la violencia, y todas las formas de maltrato infantil, incluidas la pedofilia y la pornografía infantil, así como la trata y la explotación de seres humanos. [851]

[847] Cumbre Mundial sobre la sociedad de la información, *CMSI: Plan de Acción de Ginebra*, 2003, accedido 2 de mayo de 2017, http://www.itu.int/net/wsis/docs/geneva/official/poa-es.html.
[848] Ibíd.
[849] Ibíd.
[850] Ibíd.
[851] Ibíd.

Asimismo, la Asamblea General de las Naciones Unidas aprueba la resolución No 60/1, denominada Documento Final de la Cumbre[852], en cuyo capítulo relativo a Ciencia y Tecnología señala la necesidad de utilizar las TIC para el desarrollo:

> g) Establecer una sociedad de la información centrada en las personas e inclusiva, que brinde a todos mayores oportunidades de participar en el ámbito de la tecnología digital a fin de contribuir a salvar la brecha digital, poner el potencial de las tecnologías de la información y las comunicaciones al servicio del desarrollo y hacer frente a los nuevos desafíos que plantea la sociedad de la información aplicando los resultados de la etapa de Ginebra de la Cumbre Mundial sobre la Sociedad de la Información y asegurando el éxito de la segunda etapa de la Cumbre, que se celebrará en Túnez en noviembre de 2005; a este respecto, acogemos con satisfacción el establecimiento del Fondo de Solidaridad Digital y exhortamos a que se aporten contribuciones voluntarias para su financiación. [853]

Por su parte, la Agenda de Túnez para la Sociedad de la Información, realizada en el 2005[854], señala que es necesario pasar de los principios a la acción, identificar las esferas en las que se han logrado avances y aquellas en las que aún no para reafirmar los compromisos y mejorar los mecanismos de financiación y seguimiento.

En dicho documento, consta como parte de la Agenda de Túnez para la Sociedad de la Información, dentro del criterio de *Gobernanza de Internet*, lo siguiente:

a) Sobre confianza y seguridad en el uso de las TIC:

> 39. Pretendemos crear confianza de los usuarios y seguridad en la utilización de las TIC fortaleciendo el marco de confianza. Reafirmamos la necesidad de continuar promoviendo, desarrollando e implementando en colaboración con todas las partes interesadas una cultura mundial de ciberseguridad, como se indica en la Resolución 57/239 de la Asamblea General de las Naciones Unidas y en otros marcos regionales relevantes. Esta cultura requiere acción nacional y un incremento de la cooperación internacional para fortalecer la seguridad mejorando al mismo tiempo la protección de la información, privacidad y datos personales. El desarrollo continuo de la cultura de ciberseguridad debería mejorar el acceso y el comercio y debe tener en cuenta el nivel de desarrollo social y económico de cada país y respetar los aspectos orientados al desarrollo de la Sociedad de la Información. [855]

b) Sobre las libertades y derechos humanos en Internet:

> 42. Reafirmamos nuestro compromiso con la libertad de investigar, recibir, difundir y utilizar información, en particular, para la creación, compilación y diseminación del conocimiento. Afirmamos que las medidas tomadas para asegurar la estabilidad y seguridad de Internet, combatir la ciberdelincuencia y contrarrestar el correo basura deben proteger y respetar las disposiciones en materia de privacidad y

[852] Asamblea General de las Naciones Unidas, "Resolución No. A/RES/60/1 Documento Final de la Cumbre", 24 de octubre de 2005, accedido el 12 de agosto de 2019, https://www2.ohchr.org/spanish/bodies/hrcouncil/docs/gaA.RES.60.1_Sp.pdf
[853] Ibíd.
[854] Cumbre Mundial sobre la sociedad de la información, *Agenda de Túnez para la Sociedad de la Información*, 2005, accedido 2 de mayo de 2017, accedido el 12 de agosto de 2019, http://www.itu.int/net/wsis/docs2/tunis/off/6rev1-es.html.
[855] Ibíd.

> libertad de expresión contenidas en las partes relevantes de la Declaración Universal de Derechos Humanos y en la Declaración de Principios de Ginebra. [856]

Para el 3 de noviembre de 2009, en Madrid, la Sociedad Civil consiente de la necesidad establece los Estándares de Privacidad en un Mundo Global.[857]

Asimismo, en la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid se redactó la declaración del Estándar Internacional para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal. Dicho documento demuestra la necesidad de:

> […] avanzar hacia un documento internacionalmente vinculante, que contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado, y por ello, caracterizado por las transferencias internacionales de información. Desde este momento, las autoridades de supervisión y control de la privacidad asumimos la exigente tarea de difusión y promoción desde nuestro firme compromiso de garantizar a nuestros ciudadanos una mejor protección de la privacidad y de los datos de carácter personal.[858]

Por su parte, otros organismos como la Organización para la Cooperación y el Desarrollo Económico (OCDE)[859], integrada por 37 países, cuyo objetivo es trabajar de forma coordinada para afrontar de mejor manera los retos económicos, sociales y de buen gobierno, ha considerado de suma importancia la temática de la privacidad. En este sentido, los países miembros de este organismo han señalado:

> […] necesario elaborar unas Directrices que ayudaran a armonizar la legislación nacional en materia de privacidad y, al mismo tiempo que se respetaran esos derechos humanos, evitarán las interrupciones en los flujos internacionales de datos.[860]

En tal sentido, el Consejo de la OCDE remitió las Directrices para la Protección de la Privacidad y los Flujos de Transferencia de Datos Personales, a través de una Recomendación que fue adoptada y entró en vigor el 23 de septiembre de 1980.[861]

---

[856] Ibíd.

[857] La Declaración de la Sociedad Civil, "Estándares de Privacidad en un Mundo Global", 3 de Noviembre de 2009, Madrid, accedido el 12 de septiembre de 2019, https://thepublicvoice.org/madrid-declaration/es/

[858] 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, "Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal", 5 de noviembre de 2009, Madrid, accedido el 12 de septiembre de 2019, https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf

[859] El Consejo de la Organización para la Cooperación y el Desarrollo Económico, OCDE, "Recomendación del Consejo relativa a las Directrices para la Protección de la Privacidad y los Flujos de Transferencia de Datos Personales", 23 de septiembre de 1980, accedido el 12 de septiembre de 2019, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#top

[860] Ibíd.

[861] El Consejo de la Organización para la Cooperación y el Desarrollo Económico, OCDE, "Recomendación del Consejo relativa a las Directrices para la Protección de la Privacidad y los Flujos de Transferencia de Datos Personales", 23 de septiembre de 1980, accedido el 12 de septiembre de 2019, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#top

Posteriormente, el 11 de julio de 2013, el Consejo de la OCDE adoptó una Recomendación revisada relativa a las Directrices de 1980[862]. Esta iniciativa da lugar a:

> […] un llamamiento de los Ministros en la Declaración de Seúl de 2008 sobre el futuro de la economía de Internet para evaluar las Directrices a la luz de <<la evolución de las tecnologías, los mercados y el comportamiento de los usuarios, y la creciente importancia de las identidades digitales>>. El Grupo de Trabajo de la OCDE sobre Seguridad de la Información y Privacidad (WPISP) acordó los términos de referencia para la revisión en 2011.[863]

Los principales temas recogidos en esta actualización son los relativos al enfoque basado en la gestión de riesgos y en la notificación de la violación de la seguridad de los datos, la necesidad de mejorar la interoperabilidad mundial como mecanismo que permita el libre flujo de datos entre países y el respeto de los derechos humanos, todo ello a través de estrategias nacionales y programas de gestión de la privacidad.[864]

Desde el otro lado del mundo, el Foro de Cooperación de Asia Pacífico, APE nació en 1989 por iniciativa de Australia y Japón y tiene por objetivo promover el bienestar y el crecimiento económico a través del libre mercado y la inversión en la región. Dicho organismo dictó el Marco de privacidad del foro de cooperación económica Asia Pacífico, APEC, motivado principalmente en:

> La falta de confianza del consumidor hacia la privacidad y seguridad de transacciones en línea y redes de información es un elemento que puede impedir a las Economías Miembro, obtener todos los beneficios del comercio electrónico. Las Economías de APEC se dan cuenta que una parte de los esfuerzos clave para mejorar la confianza del consumidor y asegurar el crecimiento del comercio electrónico, debe ser la cooperación para balancear y promover la protección de la privacidad de la información y el libre flujo de información en la región Asia Pacífico.[865]

Este marco normativo está inspirado en la Directivas de 1980 de la OCDE, y tiene como propósito proveer de los principios básicos para la recolección de información personal en las transferencias electrónicas entre los países miembros.

Por su parte, el Grupo de Trabajo de Ingeniería de Internet, IETF, organización internacional, que a través de propuestas y estándares, modificaciones, parámetros y documentos técnicos relevantes, tiene por objetivo contribuir a la arquitectura y funcionamiento correcto de Internet. En julio de 2013 dicta el documento No. RFC 6973 denominado Consideraciones de Privacidad para Protocolos de Internet, que tiene por finalidad:

---

[862] Consejo de la Organización para la Cooperación y el Desarrollo Económico, OCDE, "The OECD Privacy Framework", 2013, accedido el 12 de septiembre de 2019, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[863] *Ibíd*.

[864] Consejo de la Organización para la Cooperación y el Desarrollo Económico, OCDE, "The OECD Privacy Framework", 2013, accedido el 12 de septiembre de 2019, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[865] Foro de cooperación económica Asia Pacífico, "Marco de privacidad del foro de cooperación económica Asia Pacífico, 2005, Traducido del inglés, el idioma original del documento, por la Secretaría de Economía del Gobierno de México. Información tomada de "APEC Privacy Framework" accedido el 12 de septiembre de 2019, https://sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf

> […] proporciona una guía detallada a los diseñadores de protocolos acerca de ambos cómo considerar la seguridad como parte del diseño del protocolo y cómo informar lectores de especificaciones de protocolo sobre cuestiones de seguridad. Este tiene la intención de proporcionar un conjunto similar de directrices para teniendo en cuenta la privacidad en el diseño del protocolo.[866]

Pero además, la Unión Internacional de Telecomunicaciones (UIT) organismo de las Naciones Unidas dedicado a regular las telecomunicaciones a escala mundial desde 1865 y tiene por finalidad dictar recomendaciones, agrupados en "Series" por tema que permiten mantener una homologación y organización adecuada de la infraestructura de telecomunicaciones. Desde el ámbito de su competencia, este organismo ha dictado algunas recomendaciones sobre el tema de privacidad y protección de datos personales.

En el documento denominado *Trends in telecommunication reform 2013. Transnational aspects of regulation in a networked society*[867], la ITU hace recomendaciones relativas a la aplicación en la nube de la protección de datos y las leyes de privacidad.

En otro de los informes titulado *Quality of Service Regulation Manual,* emitido en 2017, existen recomendaciones sobre protección al consumidor y su privacidad.[868]

En el título *Powering the Digital Economy, Regulatory Approaches to Securing Consumer Privacy, Trust and Security*[869] dictado en el 2018 se hace una exploración de la privacidad en línea, de la confianza y seguridad a nivel mundial y global. Además, se explica los modelos entender los modelos de negocio de datos en línea y los mercados de datos. Asimismo, se analizan los modelos que permiten garantizar la protección, privacidad y confianza, un enfoque sobre la identidad digital en el marco de la protección de datos personales y la seguridad de datos.

Con las citas que anteceden, queda demostrado el interés de los grupos técnicos sobre esta temática, es decir, ya no se analiza el tema únicamente desde una perspectiva económica o de desarrollo, conforme el modelo de la OCDE o de APEC, sino relativa a medidas técnicas y estándares básicos que garanticen una Internet eficiente, sostenible y funcional, recalcándose el enfoque de garantía de derechos y democracia que consta en estos documentos.

Finalmente, la Resolución aprobada por la Asamblea General de las Naciones Unidas, el 25 de septiembre de 2015 No. 70/1 denominada Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible propone las líneas de acción que deberán ser implementadas en los siguientes años y entre las cuales la protección de los derechos humanos y el desarrollo del ecosistema digital plantean como supuestos evidentes a la

[866] Grupo de Trabajo de Ingeniería de Internet, IETF, "Documento No. RFC 6973 <<Consideraciones de Privacidad para Protocolos de Internet>>", 2013, accedido el 12 de septiembre de 2019, https://tools.ietf.org/html/rfc6973

[867] International Telecommunication Union, ITU, "Trends in telecommunication reform 2013, Transnational aspects of regulation in a networked society", 2013, accedido el 12 de septiembre de 2019, http://handle.itu.int/11.1002/pub/807b3f0a-en

[868] International Telecommunication Union, "Quality of Service Regulation Manual", 2017, accedido el 12 de septiembre de 2019, http://handle.itu.int/11.1002/pub/8108e11f-en

[869] International Telecommunication Union, "Powering the Digital Economy, Regulatory Approaches to Securing Consumer Privacy, Trust and Security", 2018, accedido el 12 de septiembre de 2019, http://handle.itu.int/11.1002/pub/8123e537-en

privacy o a la protección de datos personales como un habilitante importante para el desarrollo de una economía digital.[870]

2. Armonización de la protección de datos personales en América Latina

A continuación se analizará los principales instrumentos internacionales que orientan a los países latinoamericanos respecto de la privacidad, intimidad, *habeas data*, que son aquellos derechos primigenios desde los que nace el derecho a la protección de datos personales. Anotándose que, pese a la existencia de estos instrumentos ninguno de ellos desarrolla el derecho autónomo e independiente a la protección de datos personales, sino que su enfoque es limitado a la normativa de primera generación; esto es a defender los datos personales de injerencias arbitrarias: la perspectiva de la intimidad y la privacidad en la era digital. En este sentido:

> [...] la protección de la privacidad es un derecho fundamental reconocido por las Naciones Unidas que protege la libertad individual, la libertad de expresión, la intimidad y la dignidad personal. Este derecho contiene dentro de sí la protección de datos y la figura del *habeas data*, según afirma la propia Organización de Estado Americanos. El Consejo de Europa lo define como un derecho fundamental. Por su parte la Declaración Universal de Derechos Humanos y el pacto Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos definen a la privacidad como un derecho: nadie será objeto de injerencias arbitrarias o ilegales a su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su horna y reputación.[871]

En este sentido, se examinará los principales instrumentos que permiten contextualizar las decisiones de los principales organismos internacionales, cuyas decisiones afectan a un gran número de países latinoamericanos, entre ellos el Ecuador: a) los 21 informes anuales de la relatoría especial para libertad de expresión, desde 1998 hasta 2019; b) las resoluciones de la Corte Interamericana de Derechos Humanos sobre vida privada, intimidad y honra que si bien no han desarrollado un contenido específico nos muestra la realidad del desarrollo análisis de estos derechos fundamentales; c) las recomendaciones de la Organización de Estados Americanos (OEA) en materia de protección de datos personales y privacidad, que se materializa en cuatro documentos: el primero la Declaración de Principios sobre Libertad de Expresión; el segundo sobre privacidad y protección de datos presentado por David P. Stewart en febrero de 2014; el tercero, denominado *Privacy and Data Protection* presentado en julio del mismo año; y, el cuarto, la Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas dictada por el Comité Jurídico Interamericano el 25 de marzo de 2015, que establece 12 principios orientadores para los Estados

[870] Asamblea General de las Naciones Unidas, Resolución No. 70/1. Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible, 2015, accedido el 14 de septiembre de 2019, https://unctad.org/meetings/es/SessionalDocuments/ares70d1_es.pdf

[871] A. GARCÍA GONZÁLEZ Y OTROS, *Protección de datos y Habeas Data: Una visión desde Iberoamérica*, Agencia Española de Protección de Datos (Madrid: Agencia Española de Protección de Datos, 2015), 10.

miembros;[872] y d) varias resoluciones dictadas por las Naciones Unidas sobre el Derecho a la Privacidad en la Era Digital[873] y similares.

Finalmente, aquellas iniciativas como los Estándares Iberoamericanos de Protección de Datos Personales para Latinoamérica.

2.1 Informes anuales Relatoría Especial para la Libertad de Expresión

En octubre de 1997, durante el 97º Período de Sesiones, la Corte Interamericana de Derechos Humanos (CIDH), por decisión unánime de sus miembros, fue creada la Relatoría Especial para la Libertad de Expresión. Es una oficina permanente e independiente, encargada de velar por la defensa del derecho a la libertad de pensamiento y de expresión, entendido como aquel que permite la consolidación y desarrollo del sistema democrático, así como en la protección, garantía y promoción de los demás derechos humanos.

La Relatoría Especial para la Libertad de Expresión, preocupada por el derecho fundamental a la intimidad y a la vida privada, ha realizado precisiones en sus distintos informes anuales. Además, analiza la realidad de los países miembros de la Organización de Estados Americanos para exhortarlos a proteger, tanto el derecho a la libertad de expresión como la intimidad, la privacidad y el *habeas data*, lo que será materia del extracto de información que sigue a continuación.

2.1.1 Informe 1998

La Comisión Interamericana de Derechos Humanos, ante la realidad de la época en la cual cientos de periodistas alrededor del mundo eran asesinados, amenazados y en general amedrentados por los gobiernos o grupos de poder, decidió crear la Relatoría Especial para la Libertad de Expresión. Este órgano goza de independencia y funciona bajo el marco legal sobre el que opera la CIDH.

La Relatoría cumple con el objetivo de estimular de manera preferente la conciencia por el pleno respeto a la libertad de expresión en el hemisferio. Para esto desarrollará cuatro actividades fundamentales: primero, la elaboración de informes generales y especiales; segundo, la creación de una red que permita una protección efectiva en temas relacionados a la libertad de expresión; tercero, la realización de vistas que permitan verificar la situación de los países en la materia; finalmente, el fomento y promoción del respeto al derecho.

Dentro del informe se hace una reseña de la jurisprudencia desarrollada por el sistema interamericano de derechos humanos en materia de libertad de expresión; dentro de esta, se hace un análisis del caso chileno, en donde el Gobierno consideró que la honra

[872] OEA, "OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo", 2009, accedido 26 de mayo de 2018, http://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo.asp.

[873] Asamblea General de las Naciones Unidas, "Resolución A/C.3/68/L.45/Rev.1 sobre el Derecho a la Privacidad en la Era Digital", 2013, accedido 26 de mayo de 2018, http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1&referer=http://www.proteccionndedatos.org.mx/2013/12/resolucin-naciones-unidas-derecho-privacidad-digital/&Lang=S.

puede en algunos entrar en conflicto con la libertad de expresión; además se establece que el Estado debe brindar los mecanismos de protección necesarios para proteger a sus habitantes de cualquier violación del derecho a su privacidad.

Al respecto la Corte considera que la visión chilena es inaceptable, pues no se debe dar a un derecho mayor jerarquía que a otro, ya que reconociendo que los derechos a la honra y la privacidad tienen mayor *status* que la libertad de expresión, se permitiría la censura previa, la cual está totalmente prohibida.[874]

El *habeas data* es el mecanismo fundamental para evitar la difusión y divulgación, de datos sensibles o errores que puedan afectar la reputación, intimidad u otros derechos humanos.

2.1.2 Informe 1999

Dentro del informe se hace especial referencia al derecho a la información en poder del Estado y al *habeas data*, teniendo como eje fundamental la recomendación de reformar las leyes en este ámbito. La realidad que enfrenta el hemisferio no ha cambiado, el acoso a periodistas sigue siendo una constante y los Estados no han implementado medidas para sancionar y evitar que esto siga ocurriendo; además, se ha identificado que la situación del género femenino es desventajosa en el ejercicio del derecho a la libertad de expresión. Finalmente, se hace una relación de este derecho con el internet.

Se hace un estudio del derecho de acceso a la información y del *habeas data*, en donde se establece que el primero es un pilar fundamental de la democracia representativa, pues contribuye al control de la gestión estatal. Este constituye un mecanismo eficaz para combatir la corrupción y aumentar la transparencia de los actos de gobierno.

El *habeas data* es una garantía que permite que las personas accedan a la información sobre sí mismas o sus bienes que se encuentran contenidas en bases de datos o registros públicos y privados, y en el supuesto de que fuere necesario, actualizarla o rectificarla. Se hace un especial énfasis en que su importancia ha incrementado desde que las TIC se han implementado en el diario vivir de las personas, pues estas hacen que la recopilación de datos e información sea más sencilla.

En ambos casos es necesario que los países miembros incorporen dentro de sus legislaciones procesos rápidos, eficaces, simples y de bajo costo, ya que como se explicó con anterioridad, la tecnología y su desarrollo han hecho muy sencilla la recopilación de datos e información; además, permiten su transferencia, siendo necesario poder acceder, rectificar y actualizar la misma de manera eficiente.[875]

2.1.3 Informe 2000

[874] OEA, "Informes Anuales, OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo", 2009, accedido 20 de noviembre de 2017, http://www.oas.org/es/cidh/expresion/informes/anuales.asp.
[875] *Ibíd.*

Este año marca el inicio del siglo XXI, siendo necesario identificar los problemas que afectan al hemisferio en materia de libertad de expresión, la justicia social, el desarrollo sostenible y el pleno respeto a los derechos de las personas son los principales desafíos de la época. La corrupción es una realidad que afecta gravemente a los países miembros, siendo necesario desarrollar dentro del informe un estudio sobre los mecanismos de control y garantías como el derecho de acceso a la información y el *habeas data*, que representan un límite a la actividad estatal.

El capítulo II comprende la Declaración de Principios sobre Libertad de Expresión, aprobada por la Comisión Interamericana de Derechos Humanos en octubre 2000, en el 108 Período Ordinario, en el cual no solo se hace mención de los principios, sino que además la Relatoría hace una interpretación de cada uno.

Principio 3. *Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla.*

Este principio se refiere a la acción de *habeas data*. Esta acción prevé tres ejes fundamentales: el primero es el derecho a su privacidad, es decir, evitar injerencias de terceros en la misma; el segundo hace referencia al derecho a acceder a información sobre sí misma, a modificar, anular o rectificar la misma, cuando se trate de datos sensibles, falsos, tendenciosos o discriminatorios; y el tercero, el derecho de usar esta acción como un mecanismo de control y fiscalización.

Esta acción permite la efectivización de varios derechos como la privacidad, el honor, la identidad, la propiedad y la fiscalización. Su importancia ha incrementado con el desarrollo de la tecnología, cuyo uso continuo ha facilitado la recopilación, tratamiento y transferencia de información, siendo inminente garantizar procesos que permitan el acceso rápido a la información, para que en caso de requerirlo este pueda modificarse o actualizarse.

Esta acción también prevé obligaciones para los titulares de bases de datos, como el usar los datos para los objetivos específicos y explícitos establecidos; y garantizar la seguridad de los datos contra el acceso accidental, no autorizado o la manipulación. En los casos en que entes del Estado o del sector privado hubieran obtenido datos en forma irregular y/o ilegal, el peticionario debe tener acceso a dicha información, inclusive cuando esta sea de carácter clasificada (textual).

El *habeas data* es una garantía que permite el control a las actividades del Estado, siendo necesario implementar procesos eficientes, evitando la obstaculización en el acceso a la información, siendo necesario que estos mecanismos sean simples y de bajo costo. Asimismo, es necesario que

> […] para el ejercicio de dicha acción, no se requiera revelar las causas por las cuales se requiere la información. La mera existencia de datos personales en registros públicos o privados es razón suficiente para el ejercicio de este derecho. [876]

[876] *Ibíd.*

Principio 10. *Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada sólo a través de sanciones civiles, en los casos en que la persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en estos casos, debe probarse que en la difusión de las noticias el comunicador tuvo intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas.*

Bajo este principio se genera el debate sobre la revisión de leyes internas que contengan el delito de calumnias e injurias, que si bien en el deber ser tienen como objetivo proteger el honor, el buen nombre y la imagen de las personas, son utilizadas como mecanismos para coartar la libertad de expresión, sobre todo en los casos en que grupos de poder están involucrados.[877]

De otro lado, el principio 11 de la Declaración de Principios sobre Libertad de Expresión de la CIDH apuntala lo sostenido en el principio 10 cuando determina que:

> Los funcionarios públicos están sujetos a un mayor escrutinio por parte de la sociedad. Las leyes que penalizan la expresión ofensiva dirigida a funcionarios públicos generalmente conocidas como 'leyes de desacato' atentan contra la libertad de expresión y el derecho a la información. .[878]

De esta manera la privacidad no puede ser límite de acceso a la información ni a la investigación periodística para el ejercicio de la libertad de expresión.

2.1.4 Informe 2001

En los informes anteriores se ha establecido que la función principal de la Relatoría Especial de Libertad de Expresión tiene como objetivo principal proteger y promover la observancia de este derecho. Dentro del informe del año 2001 se ha contemplado hacer un análisis de la situación y realidad de los países del hemisferio de los últimos tres años, en el cual se ha podido constatar que si bien se ha evolucionado en el tema todavía se siguen presentando problemas debido a la falta de compromiso de los Estados a la hora de brindar mecanismos efectivos para garantizar el derecho a la libertad de expresión.

Específicamente, se ha hecho un análisis sobre la acción de *habeas data* en el hemisferio y su estado actual dentro de las legislaciones internas de cada país.

El *habeas data* es una acción que garantiza la transparencia de los actos de gobierno, además del derecho de acceso a la información pública.

El informe se analizó la legislación y las prácticas con relación a esta acción en los países que conforman la Organización de Estados Americanos. A cada uno se le envió un requerimiento de responder un cuestionario, del cual de los 35 países solo 10 respondieron; estos dieron como resultado que si bien el *habeas data* está previsto en el

[877] *Ibíd.*
[878] *Ibíd.*

ordenamiento jurídico, su lenguaje es ambiguo y no permite en la práctica hacer efectivos los derechos que garantiza.

Esta acción protege a las personas en relación con información abusiva, inexacta o perjudicial; garantiza el acceso a datos personales, contenidos, en bases públicas o privadas con el objetivo de que en caso de ser necesario estos sean actualizados, rectificados, anulados o cancelados.

El *habeas data*, además, permite que las personas puedan efectivizar el derecho de mantener su vida privada, y logra ser un mecanismo de control o fiscalización.

La privacidad es el derecho que tienen las personas a preservar su vida privada del marco social claramente reconocido por la ley. Muchas veces, las vulneraciones a este derecho vienen dadas por la búsqueda y difusión de información, por lo que la Relatoría ha concluido que si bien se debe garantizar este derecho y el de la reputación, estos deben ser armónicos con el derecho a la libertad de expresión para evitar limitarlo o restringirlo.

En la práctica se ha definido el *habeas data* como el derecho a la verdad, ya que se ha usado como un mecanismo de fiscalización en la investigación de violaciones de derechos humanos ocurridas durante las dictaduras militares en el hemisferio, siendo un instrumento de control para entidades de seguridad e inteligencia en la verificación sobre la legalidad en la recopilación de información personal de los ciudadanos.

Finalmente, la relatoría recomienda que los países se adapten a una visión estandarizada respecto de la acción del *habeas data*, con la finalidad de armonizar la legislación dentro del hemisferio.[879]

2.1.5 Informe 2002

Dentro de este informe se han destacado el valor fundamental del derecho a la libertad de expresión como un elemento esencial de todos los Estados democráticos, que si bien es cierto se ha debatido sobre su contenido, su inclusión dentro de los ordenamientos jurídicos ha sido ampliamente reconocida. Dentro de este informe no se encuentra detallado el contenido de acción de *habeas data*, pero si se habla sobre privacidad.

Se ha determinado que la privacidad y el honor muchas veces son contrarios a la libertad de expresión; en este sentido los países prevén dentro de su ordenamiento jurídico la sanción por delito de calumnias e injurias.

Este tipo penal muchas veces es usado como un arma a favor de grupos de poder en contra de periodistas que han intentado investigar sobre actos de corrupción o de falta de transparencia.

La relatoría ha concluido que las leyes que garantizan el derecho a la privacidad y el honor no deben limitar o restringir la difusión e investigación de información de interés

[879] *Ibíd.*

público; además, intenta promover la protección del honor mediante sanciones civiles no penales.[880]

2.1.6 Informe 2003

Durante los cincos años de vigencia de la Relatoría para la Libertad de Expresión se ha destacado que este derecho es indispensable para la existencia de una sociedad democrática; además, permite el desarrollo económico y ayuda a evitar los actos de corrupción. La acción de *habeas data* en el hemisferio está contemplada en diversas legislaciones; algunos países la asemejan a la acción de amparo, pero esencialmente esta garantiza el acceso a la información personal contenida en bases de datos públicas o privadas, con la finalidad de que en los casos que se ameritan, esta información personal sea suprimida, actualizada o rectificada.

La privacidad y el honor son derechos fundamentales de los seres humanos, y en la práctica se han presentado diversos casos en los cuales la libertad de expresión se encuentra en conflicto con los mencionados derechos; en consecuencia, la relatoría ha manifestado la necesidad de balancear y armonizar estos derechos, pues deben de coexistir y no mantenerse en conflicto.

Finalmente, la recomendación de la relatoría es la creación de sanciones civiles para los casos en que el honor y la reputación se vean afectados, siendo necesaria la despenalización de los delitos de calumnias e injurias.[881]

2.1.7 Informe 2004

Dentro de este informe se ha podido evidenciar que la situación en los países que conforman la Organización de Estados Americanos sigue manifestando problemas en contra de periodistas como agresiones, asesinatos, secuestros, desapariciones, entre otros. Si bien se ha avanzado en el desarrollo y mejora de legislaciones garantes de este derecho, se sigue usando el ordenamiento jurídico como un medio para sancionar y castigar actos de difusión e investigación de información.

Dentro del informe no se desarrolla a la acción del *habeas data*, pero si se habla de la protección a la privacidad que en general manifiesta la necesidad de implementar medidas que no restrinjan ni limiten la investigación y difusión de interés público.

Además, se analiza la protección a la reputación y se manifiesta que la forma adecuada para su garantía es la inserción de sanciones civiles.[882]

2.1.8 Informe 2005

Dentro de este informe, la Relatoría considera que el derecho a la libertad de expresión no solo es fundamental, sino que también es una garantía que permite asegurar la

[880] *Ibíd.*
[881] *Ibíd.*
[882] *Ibíd.*

protección de todos sus otros derechos. Se considera que el estado actual implica que los países contemplen medidas excesivas para restringir el mismo; lo principal es que se ha desarrollado un progreso en el contenido del *habeas data* se refiere. (4)

La Relatoría determina que el *habeas data* tiene implícito el derecho que tienen todas las personas a acceder no onerosamente a información sobre ella y sobre sus bienes que se encuentren en bases de datos o en registros públicos y privados; consecuentemente el derecho a actualizar, corregir o enmendar dicha información. (64)

Respecto a la privacidad, se sigue manteniendo la postura de que las leyes en esta materia no deben limitar o restringir la búsqueda, difusión o investigación de información de interés público.[883]

2.1.9 Informe 2006

Este año fue violento para el periodismo en la región pues 19 personas fueron asesinadas por motivos del ejercicio de actividades periodísticas, dando como resultado que este informe abarque temas sobre impunidad para este tipo de situaciones; además, se ha evidenciado que estas circunstancias han generado la autocensura, dando como resultado la necesidad de analizar el derecho a la vida y los procesos penales previstos en las legislaciones internas de cada país. (4)

Consecuentemente este informe no desarrolla temas como la acción de *habeas data* y privacidad; sin embargo, se habla de la relación entre el derecho a la libertad de expresión y el derecho al honor.

Las ofensas al honor que se derivan de la investigación o difusión de información de interés público, no deben ser sancionadas penalmente pues esta práctica impacta negativamente la democracia. (9) Los periodistas deben poder ejercer su labor sin la preocupación de ir a la cárcel por ello, siendo la rectificación y las sanciones civiles, la manera en que debe darse la protección. (20)

Es una de las recomendaciones de la Relatoría el derogar de las legislaciones, los delitos de desacato, calumnias e injurias, cuando se refiere a la difusión e investigación de información de interés público.[884]

2.1.10 Informe 2007

El año 2007 fue violento nuevamente. Se reportaron 16 personas asesinadas en el ejercicio de su actividad periodística y al menos hubo 200 casos de agresiones y amenazas en contra de personas que ejercían su derecho a libertad de expresión. Estos actos siguen siendo impunes en los países que conforman la Organización de Estados Americanos. En consecuencia, dentro de este informe se han analizado las acciones que deben tomarse para evitar que sigan ocurriendo estos episodios.

[883] *Ibíd.*
[884] *Ibíd.*

En ese contexto, dentro del informe se ha hecho un estudio y desarrollo de las legislaciones internas de cada país para evidenciar que las acciones legales no son suficientes para garantizar los derechos de los periodistas, pero nada se menciona acerca de la *habeas data*, privacidad y el honor.[885]

2.1.11 Informe 2008

Durante los diez años de vigencia de la Relatoría Especial para la Libertad de Expresión se han dado significativos avances de lo que a este derecho se refiere; sin embargo, se siguen presentando a la hora de promover, garantizar y respetar este derecho. Sigue siendo uno de los objetivos principales establecer mecanismos que aseguren el fortalecimiento de la democracia, el bienestar y progreso de los habitantes. (4)

La Relatoría considera que la acción de *habeas data* es el mecanismo fundamental para evitar la difusión y divulgación de datos sensibles o errores que puedan afectar la reputación, intimidad u otros derechos humanos. Asimismo, las legislaciones deben proveer que para el acceso no es necesario que el titular de la información justifique el porqué, sino que basta con la intención de acceder a un dato personal para que la persona pueda hacerlos. (223)

También se indica que la privacidad y el honor siguen presentando conflictos en relación con la libertad de expresión, y se sigue manteniendo la postura de que estos derechos no pueden limitar o restringir la investigación y difusión de interés social, que si bien es cierto es necesario brindar protección a la reputación de las personas, las sanciones penales no son las respuestas para evitar acciones en contra de estos derechos, sino más bien la inclusión dentro del campo civil los mecanismos necesarios para la efectivización del derecho al honor de los seres humanos. (223)

Finalmente, la Relatoría recomienda la promulgación de la normativa que permita el acceso efectivo a la información personal a todos los ciudadanos (233).[886]

2.1.12 Informe 2009

Dentro de este informe se sigue poniendo especial énfasis en el análisis de la situación que enfrentan los países en relación con asesinatos, agresiones y amenazas en contra de periodistas, ya que no se habla solamente de impunidad sino de prevención.

También se desarrolla el derecho de acceso a la información personal y se manifiesta que las personas tienen el derecho a acceder a la información sobre sí mismas o sus bienes en forma expedita y numerosa, ya sea que este contenido se encuentre en base de datos, registros públicos o privados, o si sea el caso tiene el derecho a actualizarla o rectificarla. Se manifiesta, además, que los sujetos tienen derecho a la actividad y a la honra, dando como resultado que nadie puede ser sujeto a injerencias en su vida privada.

---

[885] *Ibíd.*
[886] *Ibíd.*

Se mantiene la postura de que no por hacer efectivo el derecho a la privacidad y el honor se debe limitar a la libertad de expresión y que, además, las legislaciones deben de prever únicamente civiles en los casos que estos derechos se vean afectados.[887]

2.1.13 Informe 2010

Sigue siendo una preocupación de la Relatoría Especial para la Libertad de Expresión las situaciones de agresión, amenazas y asesinatos a periodistas en el hemisferio, por lo que en este informe se puso especial énfasis en el análisis de mecanismos que permitan garantizar el efectivo goce del derecho a la libertad de expresión en los países que pertenecen a la Organización de Estados Americanos. (8)

El *habeas data* comprende el derecho que tienen todas las personas de acceder a información sobre sí mismas o sobre sus bienes contenida en bases de datos o registros públicos y privados, y en caso de ser necesario actualizar rectificar o suprimir la misma. (81) La privacidad y la honra son derechos fundamentales de las personas, y se siguen dando casos en los cuales estos entran en conflicto con la libertad de expresión, pero la postura sigue siendo la misma, se debe buscar el balance entre ellos. (135)

La privacidad y el honor para su protección no requieren medidas que limitan o restrinjan la investigación y difusión de información de interés público y tampoco medidas penalmente sancionatorias.[888]

2.1.14 Informe 2011

Dentro de este informe se evalúa la situación de libertad de expresión en el hemisferio. Sigue siendo una preocupación la situación constante de peligro que sufren los periodistas, pues son sujetos de agresiones y amenazas, en donde no solo es necesario investigar, juzgar y sancionar, sino también prevenir; pero se debe destacar lo fundamental de implementar medidas de reparación a las víctimas. (8)

La acción de *habeas data* permite a las personas acceder a toda información sobre sí mismas, o sus bienes que consten en bases de datos o registros públicos y privadas, y en caso de ser necesario actualizar, rectificar o suprimir la misma; este es un elemento esencial de la libertad de expresión y del sistema democrático. (392)

En el Capítulo III sobre el derecho al acceso a la información pública en las Américas se establecen excepciones:

> Por su parte, el artículo 18 considera como "intereses privados preponderantes" que justifican la denegatoria de información, aquellos relacionados con datos personales cuya publicidad pudiera significar una invasión de la privacidad, y la propiedad intelectual. Como ya fue advertido al estudiar disposiciones similares, algunas de las causales enunciadas presentan una notable amplitud. Por ello, mientras no se establezcan parámetros legislativos más precisos, corresponderá a las autoridades de

[887] *Ibíd.*
[888] *Ibíd.*

> aplicación concretar dichas causales en reglas claras, y precisar y justificar de manera suficiente la aplicación. (399)[889]

La visión sobre la privacidad y el honor no ha cambiado; se sigue debatiendo sobre el conflicto existente sobre estos derechos, con la libertad de expresión, y se sigue concluyendo que las leyes que protegen los mismos no deben limitar o restringir la difusión e investigación de información de interés social. Asimismo, la recomendación es la inclusión de sanciones civiles para garantizar estos derechos. (248) [890]

2.1.15 Informe 2012

El informe de este año manifiesta las preocupaciones de la Relatoría sobre el peligro que sufren los periodistas en el hemisferio. Se ha hecho un análisis de las legislaciones internas y de la jurisprudencia para determinar el estado de impunidad de cada uno. (6)

La recomendación de la Comisión que más favorece a la libertad de expresión es la de priorizar el derecho de acceso a la información pública por sobre la privacidad, en aquellos casos relativos a funcionarios públicos o personas públicas o particular involucrado por su voluntad en asuntos de interés público.

Al analizar el caso Perú, precisa que es preocupante la aplicación del delito de difamación a personas que han hecho denuncias o manifestado opiniones críticas respecto de quienes ocupan o han ocupado cargos públicos.

En cuanto al caso Colombia, la Relatoría Especial manifiesta su preocupación por el hecho de que el canal solicite información sobre la vida privada de sus trabajadores o contratistas. La emisora no debe contar con esta información y tampoco puede en ningún caso hacer públicos dichos datos personales, que por cualquier razón reposen en sus archivos. (155) Asimismo, la Relatoría Especial señala su preocupación respecto de que:

> un servidor público solicite información a un medio público de comunicación, con la única finalidad de reproducir estereotipos discriminatorios que carecen de cualquier fundamento razonable, y de reforzar prácticas y políticas segregacionistas y antidemocráticas, que no sólo afectan a las personas directamente concernidas, sino a toda la sociedad en su conjunto.(155) [891]

Esta afirmación nos da razón de que la recolección y finalidad de los datos son elementos sustanciales de protección debido a que la divulgación de datos personales puede afectar la dignidad humana.

Sobre datos personales y seguridad nacional, en decisión T-1037 de 2008, del 23 de octubre de 2008, la Corte Constitucional de Colombia resolvió:

> […] el caso de una periodista a quien le habían concedido y después retirado un esquema oficial de protección el cual le había sido asignado debido a amenazas en su

[889] *Ibíd.*
[890] *Ibíd.*
[891] *Ibíd.*

> contra. Durante el proceso de tutela (amparo) se pudo advertir que el escolta asignado adelantó actividades de inteligencia de forma ilegal y sin conocimiento de la periodista. En el asunto de tutela, orientado inicialmente a discutir sobre el restablecimiento del esquema de seguridad, la Corte advirtió también la vulneración del derecho de la periodista a conocer y controlar su información personal o *habeas data*. En este contexto, la Corte reconoció el derecho de acceso a la propia información personal en archivos de inteligencia del Estado y le ordenó a la agencia de seguridad del Estado suministrar toda la información personal que tuviera sobre la periodista, en los siguientes términos: "en principio y salvo la existencia de una ley que establezca lo contrario, la información que repose en los archivos del Estado es pública. Sin embargo si esta información se refiere a los datos privados, íntimos o reservados de una persona y los mismos no son de relevancia pública, en principio, no pueden ser ni capturados y archivados ni divulgados, pues se encuentran protegidos por el derecho a la intimidad. No obstante, si el dato reposa en un archivo oficial, la persona titular de dicho dato, salvo expresa reserva legal, tiene derecho fundamental de acceso a dicha información". Más adelante, concluye la Corte: "[e]n efecto, una persona que ha solicitado y obtenido la protección del Estado por encontrarse en una circunstancia de riesgo extraordinario tiene derecho constitucional fundamental a conocer integralmente toda la información que sobre ella repose en los archivos de inteligencia y todos los reportes elaborados por las personas encargadas de protegerla, con excepción de aquella que haga parte de una investigación judicial [que] esté sometida a la reserva del sumario". (69) [892]

El criterio para captura, archivo y divulgación de datos personales es la relevancia pública. En cuanto a la información propia que conste en un archivo oficial, el titular tiene derecho fundamental de acceso a dicha información, a menos que estos sean parte de la reserva de un proceso de investigación judicial.

En este sentido, el informe 2012, respecto del *habeas data*, mantiene lo dicho anteriormente. Esto es que, hace referencia al derecho que tienen todas las personas de acceder a información sobre sí mismas o sus bienes, contenida en bases de datos o registros públicos o privados; y en caso de ser necesario actualizar, suprimir o rectificar la misma.

En lo relativo al caso República Dominicana, la Relatoría Especial apoya la Jurisprudencia sobre derecho a acceder a información relacionada con salarios e ingresos de servidores públicos o contratistas provenientes de recursos públicos, contenida en sentencia No. TC/0042/12, dictada por el Tribunal Constitucional de República Dominicana el 21 de septiembre de 2012 que señala lo siguiente:

> Se confirmó una sentencia de amparo que ordenó entregar toda la información relativa a la nómina de los asesores de la Cámara de Diputados, contentiva de nombres, apellidos, cargos y sueldos. El Tribunal Constitucional enfatizó la importancia del derecho de acceso a la información pública y la obligación de trasparencia del Estado. Asimismo, realizó una ponderación entre el derecho de acceso a la información, y los derechos a la intimidad de los funcionarios públicos y a la protección de sus datos personales. Además, en consonancia con los estándares interamericanos en la materia, determinó que este último sólo puede restringir el derecho de acceso a la información pública de forma excepcional, pues de lo contrario se "despojaría a la ciudadanía de un mecanismo esencial para el control de la corrupción en la Administración Pública". (436) [893]

[892] *Ibíd.*
[893] *Ibíd.*

Finalmente, los casos de conflicto con la libertad de expresión la ley no puede restringir o limitar la investigación, difusión de información de interés social; los ordenamientos jurídicos tampoco pueden contener sanciones penales para proteger estos derechos.[894]

El informe del año 2012 es el primero que establece como factor de protección de la dignidad humana, la confidencialidad de los datos personales y establece como aquellos que se refieren a funcionarios públicos. Ya que en este caso, prima el derecho a la libertad de expresión por encima del interés individual del titular a su privacidad. Asimismo, desarrolla la comprensión de que el derecho de acceso a la información personal por parte del titular es un mecanismo que permite el control del poder estatal, en especial cuando el Estado posee información por concepto de seguridad nacional.

2.1.16 Informe 2013

La realidad en Latinoamérica evidencia que los gobiernos de cada país incurren en mayores lesiones a la libertad de expresión; los asesinatos agresiones y amenazas se han elevado significativamente, la corrupción está sumamente arraigada, siendo uno de los objetivos principales de la Relatoría recomendar a los Estados medidas que puedan garantizar la democracia y la transparencia. (2)

En cuanto a la acción de *habeas data* ha sido reconocida y desarrollada en la mayoría de los países de la región. Sigue siendo considerada una garantía para el acceso a la información personal, su actualización, rectificación o eliminación; además, constituye una garantía para la transparencia de los actos de gobierno, respecto de los datos personales que recoge de sus ciudadanos. (135) Asimismo, varios países han incorporado en sus legislaciones al derecho a la protección de datos personales, y al *habeas data* como mecanismo para hacerlo efectivo. Uno de los citados casos es el del Ecuador.

Sobre el derecho a la privacidad y el honor, se sigue estableciendo que en los casos de conflicto con la libertad de expresión, la ley no puede restringir o limitar la investigación, difusión de información de interés social; los ordenamientos jurídicos tampoco pueden contener sanciones penales para proteger estos derechos.[895]

El caso de mayor relevancia en el citado informe es el relativo a Estados Unidos, la Relatoría Especial se cuestiona el alcance de distintos programas secretos de vigilancia que estarían siendo implementados por el Gobierno de los Estados Unidos[896],

[894] *Ibíd.*
[895] *Ibíd.*
[896] El sistema informático conocido como PRISM facilitaría el acceso a la NSA y a la Oficina Federal de Investigación a datos de comunicaciones digitales o metadatos e incluso se afirma que al contenido mismo del mensaje transferido, de nueve proveedoras de servicios de Internet, entre ellos, Microsoft, Google, Facebook, Apple, Yahoo y Skype. Extracción de información que se afirma se ha realizado sin orden judicial individualizada, en aquellos casos en los que el objetivo de vigilancia no es una "persona de Estados Unidos" y se podría creer de manera razonable que no se encontraba en territorio estadounidense al momento de la recopilación de la información. Según la información revelada, la NSA también utilizaría dos programas, UPSTREAM y XKEYSCORE para acceder a grandes cantidades de información, buscar y analizar datos de la actividad en Internet de un individuo. (403 y 404) (…) las agencias de inteligencia podrían monitorear las comunicaciones "sobre" sus objetivos extranjeros, lo que habría sido interpretado para permitir escanear el contenido de cualquier comunicación que se origine o termine en los Estados Unidos, por palabras claves relacionadas con sus objetivos. Ibíd.

amparados en la Orden del Ejecutivo No. 12333811 y la Ley de Vigilancia de Inteligencia Extranjera [Foreign Intelligence Surveillance Act] (FISA), de conformidad con las reformas introducidas a dicha ley por la sección 215 de la Ley Patriota [Patriot Act] de 2001812 y la sección 702 de la Ley de Enmiendas de 2008813.[897]

Dichos programas tienen la finalidad de obtener de forma masiva metadatos de comunicaciones telefónicas realizadas o recibidas en los Estados Unidos y por otra, el acceso a datos de comunicaciones electrónicas globales. (394) Ahora bien, el informe señala que esta práctica atenta las expectativas razonables de privacidad pues, en primer lugar, va "más allá de lo estrictamente necesario para lograr fines legítimos de seguridad nacional y generan un efecto amedrentador en el derecho de buscar, recibir y difundir información e ideas de toda índole"(410)[898]; en segundo lugar, no solo se limita a "la investigación de terrorismo, sino que también incluiría cualquier asunto relevante a los intereses externos del país"(410)[899], postura indeterminada por la cual se evidencia una recolección masiva e injustificada de datos personales; y finalmente, afecta derechos de los extranjeros que residen fuera de los Estados Unidos; que sin ser parte de una investigación penal, sus comunicaciones estarían siendo interceptadas por la NSA. Ya que, a criterio de este país bajo la Constitución de los Estados Unidos, gozan de una protección reducida. Aseveración que atenta contra la igualdad de las personas.

En este sentido, el informe describe a este tipo de vigilancia como invasiva; así mismo, reflexiona en la gravedad y puesta en riesgo de los derechos a la intimidad y a la libertad de pensamiento y expresión de las personas, e incluso considera que pudiera llegar a afectar a la propia democracia, al tenor del siguiente texto:

> […] la recolección de metadatos telefónicos invadiría igualmente expectativas razonables de privacidad. Según fue indicado, este tipo de información, recopilada en forma masiva y con el apoyo de poderosas herramientas analíticas, expondría de manera extraordinaria los hábitos y vínculos de las personas, revelando relaciones personales, condiciones de salud, conducta laboral o afiliaciones políticas o religiosas, por lo que el Estado tendría que justificar la proporcionalidad y razonabilidad de la medida, en relación con los fines que busca proteger. Asimismo, de acuerdo con la información recibida, la Sección 215 de la Ley Patriota, base legal de la recolección masiva de metadatos telefónicos, estaría siendo interpretada en sentido contrario a su lenguaje ordinario y el espíritu del legislador y los controles judiciales existentes no serían efectivos. En particular, la Comisión recibió información que sugiere que el programa tendría un gran potencial de limitar la libertad de expresión y asociación de organizaciones de derechos humanos que reciben llamadas de clientes y de informantes, actuales o potenciales, que buscan apoyo legal en casos en contra del gobierno. (400) [900]

Como corolario de este caso, el Presidente Barak Obama creó el Grupo de Revisión sobre Inteligencia y Tecnologías de Comunicación, con la finalidad de evaluar que Estados Unidos emplee:

> […] capacidades técnicas de recolección de un modo que brinde óptima protección a nuestra seguridad nacional y fomente nuestra política exterior y, al mismo tiempo, tenga en cuenta otras consideraciones en materia de políticas,

[897] *Ibíd.*
[898] *Ibíd.*
[899] *Ibíd.*
[900] *Ibíd.*

> tales como el riesgo de que se produzca una divulgación no autorizada y la necesidad de preservar la confianza pública. [901]

Este Grupo de Revisión formuló 46 recomendaciones una de las cuales hace referencia a las medidas significativas que deben desarrollarse para proteger la privacidad de las personas no estadounidenses. Y señaló que "cualquier programa que permita la vigilancia de dichas personas, aun fuera de los Estados Unidos, debería cumplir con seis limitaciones independientes" [902] que se citan a continuación:

> […] 1) deberá ser autorizado por leyes sancionadas conforme a los procedimientos estipulados o decretos ejecutivos debidamente autorizados; 2) deberá estar destinado exclusivamente a proteger intereses de seguridad nacional de los Estados Unidos o [sus] aliados; 3) no deberá tener fines ilícitos o ilegítimos, como el robo de secretos comerciales o la obtención de ventajas comerciales para industrias nacionales; 4) no deberá estar dirigido a personas que no sean de los Estados Unidos exclusivamente en razón de sus opiniones políticas o convicciones religiosas; 5) no deberá difundir información sobre personas que no sean de los Estados Unidos cuando tal información no resulte relevante para proteger la seguridad nacional de los Estados Unidos o [sus] aliados y 6) deberá estar sujeto a una atenta supervisión y al más alto nivel de transparencia que resulte consistente con la protección de la seguridad nacional de los Estados Unidos y [sus] aliados". Recomendó asimismo que "a falta de una demostración concreta y convincente, el Gobierno estadounidense debería seguir el modelo del Departamento de Seguridad Nacional y aplicar la Ley de Privacidad de 1974 de manera idéntica tanto a personas de los Estados Unidos como a aquellas que no lo sean". La Relatoría Especial señala en particular que el Grupo de Revisión recomendó que el "Congreso debería crear el cargo de Defensor de Interés Público para actuar en representación de la privacidad y las libertades civiles ante la Corte de Vigilancia de Inteligencia Extranjera" y que "se debería reforzar la transparencia de las decisiones de la Corte de Vigilancia de Inteligencia Extranjera, entre otras cosas, estableciendo evaluaciones sobre desclasificación que cumplan con los estándares vigentes". (423) [903]

Otro caso analizado en el informe 2013 es aquel relativo al uso de acciones judiciales para requerir información que permitirían identificar la fuente. Este mecanismo de abuso del derecho afecta la privacidad de la fuente y el derecho a la libertad de expresión, conforme consta descrito en el siguiente texto:

> *The Associated Press* (AP) recibió una carta de la Oficina del Fiscal de Estados Unidos para el Distrito de Columbia, en la que se le notificó que el Departamento de Justicia había obtenido los registros telefónicos de más de 20 líneas utilizadas por editores y periodistas de la agencia durante abril y mayo de 2012. Los registros incluirían llamadas realizadas desde las oficinas de AP y de las líneas telefónicas personales de varios integrantes del personal. Las acciones de recopilación habrían ocurrido sin aviso previo a la agencia de noticias o a sus periodistas" (425) La Relatoría Especial manifestó su preocupación y advirtió que este tipo de prácticas pueden afectar el ejercicio de un periodismo libre al poner en riesgo la confidencialidad de las fuentes periodísticas. (425) [904]

En cuanto al caso del periodista James Risen, obligado por orden judicial a revelar su fuente, la Relatoría Especial ha indicado en otras ocasiones que:

[901] *Ibíd.*
[902] *Ibíd.*
[903] *Ibíd.*
[904] *Ibíd.*

> […] la importancia del derecho a la confidencialidad de las fuentes reside en que en el ámbito de su trabajo y a fin de proveer al público de información necesaria para satisfacer su derecho a recibir información, los periodistas realizan un importante servicio al público cuando recaban y difunden información que no sería divulgada si la reserva de las fuentes no estuviera protegida. La confidencialidad, por lo tanto, es esencial para el trabajo de los periodistas y para el rol que cumplen a la sociedad de informar sobre asuntos de interés público. La Relatoría Especial recuerda al Estado la necesidad de adoptar todas las medidas necesarias para evitar poner en peligro esta garantía fundamental para el ejercicio de un periodismo libre. (432) [905]

En suma, respecto de privacidad y reserva de fuentes periodísticas, la Relatoría Especial recomienda:

> […] a) diseñar medidas de protección disponibles como resultado de estudios de riesgo integral, que atiendan la complejidad de cada caso, en consulta con el potencial beneficiario; y, b) que se garantice la continuidad del ejercicio de la actividad periodística, a través de la satisfacción de necesidades específicas como la privacidad para reunirse con sus fuentes. (84)[906]

En este año, la Relatoría Especial para la libertad de expresión de la Comisión Interamericana de Derechos Humanos dicta el informe titulado, Libertad de expresión e internet. Cuyo objetivo es orientar y promover la revisión y adopción de legislación y prácticas en los Estados de la región, sobre los principios generales de protección del derecho a la libertad de pensamiento y expresión en el entorno digital.

Ahora bien, tomando como ejemplo el caso americano, la Relatoría Especial sostiene que: "los programas de vigilancia deben ser diseñados e implementados atendiendo a los estándares internacionales en materia de derechos humanos" (415)[907], en tal virtud, establece como indispensable cumplir con los siguientes límites a continuación dispuestos:

1. *Claramente autorizadas por la ley:* Existe la necesidad de revisión general de la legislación y de establecer mayores mecanismos de transparencia y discusión pública de dichas prácticas.(414) [908] En tal sentido:

> […] los Estados deben garantizar que la intervención, recolección y uso de información personal, incluidas todas las limitaciones al derecho de la persona afectada a acceder a información sobre las mismas, estén claramente autorizadas por la ley a fin de proteger a la persona contra interferencias arbitrarias o abusivas en sus intereses privados. La ley deberá atender a un objetivo legítimo y establecer límites respecto a la naturaleza, alcance y duración de este tipo de medidas, las razones para ordenarlas, las autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación. Asimismo, la ley debe autorizar el acceso a las comunicaciones y a datos personales solo en las circunstancias más excepcionales definidas en la legislación. Cuando se invoque la seguridad

[905] *Ibíd.*
[906] Capítulo III, Violencia contra periodistas y trabajadores de medios: Estándares interamericanos y prácticas nacionales sobre prevención, protección y Procuración de la justicia. Ibíd.
[907] *Ibíd.*
[908] *Ibíd.*

> nacional como razón para vigilar la correspondencia y los datos personales, la ley debe especificar claramente los criterios que deben aplicarse para determinar los casos en los cuales este tipo de limitaciones resultan legítimas. Su aplicación deberá autorizarse únicamente cuando exista un riesgo cierto respecto de los intereses protegidos y cuando ese daño sea superior al interés general de la sociedad en función de mantener el derecho a la privacidad y a la libre expresión del pensamiento y circulación de información. (415) [909]

2. *La decisión judicial sea el mecanismo de autorización.* El juez que la dicta deberá ser independiente, y estará a cargo de ponderar de derechos, incluido el debido proceso, en cada caso puesto a su conocimiento, dentro de un test, descrito a continuación y establecer las razones por las cuales la vigilancia es la medida idónea:

> […] las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas deben ser autorizadas por autoridades judiciales independientes, que deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover (…) Los Estados deben garantizar que la autoridad judicial sea especializada y competente para tomar decisiones judiciales sobre la legalidad de la vigilancia de las comunicaciones, las tecnologías utilizadas y su impacto en el ámbito de los derechos que pueden resultar comprometidos.(165) [910]

3. *Adecuadas y efectivas garantías en contra del abuso.* En cuanto a la normativa que regula la vigilancia de las comunicaciones, el informe determina la necesidad de que en ella se determine la o las autoridades encargadas de autorizar, realizar y supervisar la procedencia y ejecución de la vigilancia, al tenor de los siguientes criterios:

> […] aplica respecto de este tema el principio de "máxima divulgación" que rige en relación a todos los actos estatales: ellos son públicos y sólo pueden reservarse del conocimiento del público bajo las más estrictas circunstancias, siempre y cuando esa reserva esté establecida por ley, busque satisfacer un objetivo legítimo bajo la Convención Americana y sea necesaria en una sociedad democrática. (166) Como lo ha señalado la Corte Europea de Derechos Humanos, un sistema de vigilancia secreta puede "debilitar o incluso destruir a la democracia bajo el pretexto de defenderla". Por ello, la Corte exige que haya "adecuadas y efectivas garantías en contra del abuso". Para determinar si ello ocurre en un caso concreto, el tribunal señaló que es necesario analizar "la naturaleza, el alcance y la duración de las posibles medidas, las razones que las justificarían, las autoridades encargadas de autorizarlas, realizarlas y supervisarlas, así como el tipo de remedios que establece el derecho interno". (167) [911]

4. *Transparencia de las instituciones públicas y privadas:* Sobre la necesidad de publicación de información global sobre el número de solicitudes de intercepción y vigilancia aprobadas y rechazadas, incluyendo la mayor cantidad

[909] *Ibíd.*
[910] *Ibíd.*
[911] *Ibíd.*

> de información posible, se ha señalado que tanto las instituciones públicas como los proveedores de servicios deberán cumplir con informar sobre "los procedimientos que ellos aplican cuando reciben peticiones de información por parte de autoridades públicas, así como información sobre, cuando menos, el tipo de requerimientos que reciben y su cantidad". (169)[912] Al tenor de lo señalado en la resolución "El derecho a la privacidad en la era digital", adoptada por consenso por los miembros de la Asamblea General de la ONU el 18 de diciembre de 2013, es indispensable "la supervisión independiente y efectiva capaz de asegurar la transparencia y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado".(170)[913] Se vuelve imperante, entonces, "la necesidad de establecer mayores mecanismos de transparencia y control, de conformidad con el derecho internacional de los derechos humanos". (395) [914]

Podemos concluir que, solo a través de la transparencia del Estado, la imparcialidad y capacitación de las autoridades, en especial de los jueces, como autorizadores de vigilancia o supervisores de que esta actividad estatal se esté ejecutando con apego a la ley; se puede mantener el delicado equilibrio entre la seguridad, la protección de los datos personales y la libertad de expresión.

En cuanto al Capítulo VI, en la parte relativa a conclusiones y recomendaciones señala que:

> La protección de la privacidad o el honor y la reputación de funcionarios públicos o de personas que voluntariamente se han interesado en asuntos de interés público, debe estar garantizada solo a través del derecho civil. (B.8.b.) [915]

De esta manera, la fiscalización ciudadana debe poder ser ejercida respecto de funcionarios públicos o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. De tal manera que, en este caso, de existir afectaciones al honor estas se resuelvan únicamente en el ámbito civil y no penal. Siempre y cuando se logre determinar que el periodista tuvo la "intención de infligir daño ya que tenía el pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas". [916]

Esta resolución marca un hito importante en el tema de la libertad de expresión en internet, pues establece la correlación inherente y directa de este derecho, con la ciberseguridad, la protección de datos personales, la imagen y la privacidad, así como la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos. (170) Sus principales consideraciones pasan a analizarse a continuación.

La Comisión Interamericana ha señalado que el derecho a la privacidad protege:

> […] al menos cuatro bienes jurídicos, que tienen una relación estrecha con el ejercicio de otros derechos fundamentales como la libertad de pensamiento y expresión. En primer lugar, el derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas. En segundo lugar, el derecho a

[912] *Ibíd.*
[913] *Ibíd.*
[914] *Ibíd.*
[915] *Ibíd.*
[916] *Ibíd.*

> gobernarse, en ese espacio de soledad, por reglas propias definidas de manera autónoma según el proyecto individual de vida de cada uno. En tercer lugar, el derecho a la vida privada protege el secreto de todos los datos que se produzcan en ese espacio reservado, es decir, prohíbe la divulgación o circulación de la información capturada, sin consentimiento del titular, en ese espacio de protección reservado a la persona. Y, finalmente, la protección de la vida privada protege el derecho a la propia imagen, es decir, el derecho a que la imagen no sea utilizada sin el consentimiento del titular. (131)[917]

Y es que, solo en un entorno en el que el ciudadano se sienta libre de amedrentamiento y de represalias, o no se percibe supervisado o vigilado, de forma directa o indirecta por parte del Estado o de particulares (170), puede ejercer su derecho a emitir opiniones; a participar en el foro público; ejercer su derecho a ser informado, sin tener que revelar su identidad, sus datos íntimos o sus fuentes; proteger el discurso anónimo (124), así como, "llamar a movilizaciones sociales, convocar a otros ciudadanos a manifestarse, organizarse políticamente o cuestionar a las autoridades, aun en situaciones de riesgo". (134) [918]

Para garantizar la libertad de expresión a través del respeto a la privacidad, el Estado debe cumplir una serie de presupuestos que pasamos a enlistar a continuación:

- Abstenerse de realizar intromisiones arbitrarias sobre información personal y comunicaciones de las personas; (23)
- Garantizar que otros actores, privados o particulares, se abstengan de realizar estas conductas abusivas; (23)
- Promover espacios anónimos en línea, libres de observación o documentación de la actividad e identidad de los ciudadanos; (23)
- El uso de servicios de autenticación en línea: proporcionales (23) y diversos (136), de tal manera que, no existan identificadores únicos o concentrados y solo se exijan la identificación en transacciones e interacciones sensibles y riesgosas, y no de manera generalizada para todos los servicios y aplicaciones; (136)
- La defensa de la privacidad de las personas debe hacerse atendiendo a criterios razonables y proporcionados que no terminen restringiendo de manera arbitraria el derecho a la libertad de expresión;
- Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público;
- El anonimato no puede proteger discursos que atentan derechos, como los relativos a pornografía infantil, propaganda a favor de la guerra o apología del odio que constituya incitación a la violencia o a genocidios. En estos casos, las autoridades judiciales están autorizadas descubrir la identidad de los posibles infractores; (135)
- Garantizarse la confidencialidad de los datos personales en línea, (137) el derecho a la privacidad como un derecho que las personas tienen tanto fuera de línea [offline] como cuando están conectados a Internet (149);
- Los Estados deben establecer regímenes legales y técnicos de protección de datos personales que regulen su almacenamiento, procesamiento, uso y transferencia;

[917] *Ibíd.*
[918] *Ibíd.*

- Fortalecer el habeas data (140), entendido como el derecho sustantivo o la medida procesal que permita al titular al acceso, rectificación o cancelación de sus datos personales, así como a conocer cuáles son los datos tratados y con qué fin se han almacenado; (139)
- Prohibir el uso de los datos personales para fines contrarios a los tratados de derechos humanos (139) y propiciar medidas para terminar con injerencias y prevenir futuros abusos; (149)
- Los Estados revisen su legislación y establezcan límites a la vigilancia de las comunicaciones en línea, atendiendo criterios de necesidad y proporcionalidad. (151)
- Garantizar la libertad para elegir servicios y plataformas a los que una persona puede acceder. (173)
- No exigir a los proveedores de servicios de Internet, determinada localización de los datos, condición que se considera una barrera de interoperabilidad y de ingreso a los mercados de nuevas plataformas y servicios, y que afecta a la libertad de expresión, pues los usuarios reducen su acceso a recursos para investigación, educación y comunicación. "La libertad de expresión y la democracia presuponen el libre flujo de información y demandan evitar medidas que generen la fragmentación de Internet". (174) [919]

En suma, la Relatoría Especial insta a los estados a respetar y proteger la libertad de expresión en el contexto de las comunicaciones digitales. Para lo cual, es indispensable mantener un equilibrio entre seguridad nacional y privacidad; entre ciberseguridad y protección de datos personales, a través de los criterios de autorización, supervisión y control de las actividades de vigilancia de un estado, así como mediante la serie de presupuestos, acciones y abstenciones que los entes públicos y privados deben cumplir en garantía de la privacidad, reconociendo que este derecho tiene relación directa con la libertad de expresión y por ende con la democracia misma.

Finalmente, como se revisó anteriormente, este informe recomienda a los Estados "establecer regímenes legales y técnicos de protección de datos personales que regulen su almacenamiento, procesamiento, uso y transferencia". De esta manera, aunque aborda la temática aun desde una visión netamente regulatoria y no lo conceptualiza como un derecho autónomo, pues a lo largo del texto menciona únicamente a la privacidad como derecho, es interesante analizar como la Relatoría Especial va perfilando la necesidad de un sistema integrado de protección, en la que el manejo adecuado de los datos personales se vuelve prioritario para un Estado.

2.1.17 Informe 2014

En el hemisferio occidental, durante el año 2014, señala que al menos 25 personas fueron asesinadas debido a que ejercían plenamente el derecho a la libertad de expresión, por lo que se mantiene el análisis sobre estas circunstancias. Se analiza el derecho a la honra, la privacidad y se define a los datos personales sensibles. (3)

Los datos personales sensibles son aquellos que se refieren al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud

[919] *Ibíd.*

física y mental, situación moral y familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, la propia imagen, la intimidad personal y familiar, o el entorno laboral de una persona.

En el tema del derecho a la privacidad y el honor, se sigue estableciendo que en los casos de conflicto con la libertad de expresión, la ley no puede restringir o limitar la investigación, difusión de información de interés social; los ordenamientos jurídicos tampoco pueden contener sanciones penales para proteger estos derechos.[920]

En el caso Argentino, la Relatoría Especial recuerda que "la neutralidad de la red es fundamental para garantizar la pluralidad y diversidad del flujo informativo" (59)[921], elementos sustanciales para garantizar el acceso a información y por ende el ejercicio a la libertad de expresión.

En cuanto a Brasil, la Relatoría Especial reconoce el contenido de la ley 12.965/2014, conocida como "Marco Civil da Internet", 23 de abril de 2014. Ya que, establece a la libertad de expresión y la protección de la privacidad como el centro de la regulación en materia de Internet, pues garantiza la inviolabilidad de las comunicaciones en línea, que solo podrán ser reveladas a terceros mediante una orden judicial; prohíbe la suspensión de la conexión de usuarios, salvo por falta de pago del servicio; establece el principio de la neutralidad de la red y limita la responsabilidad de los intermediarios cuando inhabilitan el contenido por orden judicial. (132)

En lo relativo al caso de Canadá, la Corte Suprema emitió una resolución en el caso R. v. Spencer, conforme a la cual los organismos de seguridad del Estado deben contar con orden judicial para requerir información a los proveedores de servicios de Internet acerca de sus suscriptores, en este mismo sentido se aprobó la Ley para Proteger a los Canadienses de Crímenes Online o Bill C-13. (211)

Respecto del alcance de los programas de vigilancia implementados por la Agencia de Seguridad Nacional de los Estados Unidos, NSA. Mediante el cual, el gobierno de los Estados Unidos tendría acceso masivo a datos de las comunicaciones globales, con el propósito de obtener información de inteligencia extranjera, incluidas imágenes faciales (515). El 27 de marzo, el Presidente anunció que el gobierno no debería continuar la recolección masiva de metadatos telefónicos y que esta información debería mantenerse en las compañías telefónicas, con un mecanismo legal que permita al gobierno obtener los datos a través de órdenes individuales emitidas por la Corte de Inteligencia de Vigilancia Extranjera (520).

Se reitera lo dispuesto en la Relatoría de 2013 pero añade que los "procesos de investigación que se lleven adelante y que impliquen una invasión de la privacidad autorizada por ley y ordenada por un juez competente deben respetar, además, otras garantías vinculadas al debido proceso. (525)"[922] Este elemento adicional, se convierte entonces es un marco referencial adecuado que permite establecer a la inmediación, a la contradicción, a la imparcialidad de la autoridad, entre otras, como presupuestos rectores que guíen tanto la actuación estatal como la exigibilidad del derecho por parte del titular.

[920] Ibíd.
[921] *Ibíd.*
[922] *Ibíd.*

Se puede concluir que, este informe hace hincapié en la privacidad como elemento sustancial para garantizar la libertad de expresión, ya que de no ser respetada afecta directamente la participación y generación libre y voluntaria de opinión. Por ello, establece una serie de elementos mínimos que debe contener la normativa cuando se intenta disminuir este derecho al relacionarlo con temas de investigación de delitos y de vigilancia por seguridad nacional, al tenor de lo señalado previamente en el informe 2013.

2.1.18 Informe 2015

El Informe de la Relatoría Especial de 2015 determina como uno de sus ejes centrales a la privacidad y su contraste con la libertad de expresión. En cuanto al derecho a la privacidad y el honor, se sigue estableciendo que, en los casos de conflicto con la libertad de expresión, la ley no puede restringir o limitar la investigación, difusión de información de interés social; los ordenamientos jurídicos tampoco pueden contener sanciones penales para proteger estos derechos.[923]

La declaración conjunta sobre acceso a la información, violencia contra las mujeres y la administración de justicia en las américas, de 4 de mayo de 2015, determinó que:

> […] el acceso a la información está estrechamente vinculado con el disfrute de otros derechos humanos fundamentales de las mujeres, como su derecho a la integridad personal, a la privacidad, a la protección de la familia y a vivir libres de violencia y discriminación. [924]

En este informe se analiza, por primera vez, la relación directa entre acceso a información y privacidad. Se demuestra la necesidad de su desarrollo y análisis. Se reconoce a la privacidad como un derecho que permite una verdadera igualdad de género explicitada en el ejercicio de las libertades individuales de mujeres, en especial en ámbitos de salud, reproducción y libertad sexual.

A diferencia del informe anterior, en el caso Canadá, la Ley de Privacidad Digital de 18 de junio se habilita de forma excepcional la entrega de datos personales de los usuarios sin su consentimiento o conocimiento, por parte de proveedores de servicios de Internet. Únicamente en los casos relacionados a detectar, prevenir o reprimir el fraude, o proteger a las víctimas de los delitos financieros; por cuestiones de salud o atención de personas heridas o enfermas a para informar a los familiares; para establecer, gestionar o terminar la relación de trabajo en los casos específicos que requieran el uso o la divulgación de la información. (292)

Respecto de la iniciativa *Free Basics* liderada por la organización internet.org, por la cual se entregaría internet gratuito en zonas donde no existe acceso con la condición de que solo se acceda a Facebook y a páginas sociales de esta compañía. Esta propuesta ha sido ampliamente criticada por cuanto impactaría en la neutralidad de la red, el acceso universal a internet, la privacidad, la libertad de expresión debido a los privilegios zero-

[923] *Ibíd.*
[924] *Ibíd.*

rating o tasa cero, ya que en el largo plazo "termina generando la concentración de la infraestructura y el monopolio sobre el tráfico de datos en la red"[925], así como reduce "tanto la disponibilidad de contenidos, aplicaciones y servicios en Internet, como la libertad de elección del usuario".[926]

Sobre el caso Estados Unidos, el 7 de mayo, la Corte de Apelaciones del Segundo Circuito determinó que el programa de recolección de metadatos telefónicos "excede el alcance de lo que el Congreso ha autorizado y por lo tanto viola el Artículo 215"[927] de la Ley Patriota, pues este "no puede interpretarse de manera tal que desafíe todo límite significativo". (643)[928] La Relatoría recomienda que se garantice que sea una autoridad judicial la encargada de autorizar, revisar y controlar "la legalidad de la vigilancia de las comunicaciones, las tecnologías utilizadas y su impacto en el ámbito de los derechos que pueden resultar comprometidos y que tengan suficientes garantías para ejercer sus funciones de manera adecuada".(643)[929] Finalmente, la Relatoría Especial observa que por lo menos los criterios de decisión adoptados por los tribunales deberían ser públicos.

Sobre la situación en Perú, se determina que "las causas y condiciones que habilitarían al Estado a interceptar las comunicaciones de las personas, a recoger datos de comunicación o "metadatos", o a someterlas a una vigilancia o seguimiento que invada esferas en las que tienen razonables expectativas de privacidad" [930] deben establecerse a través de leyes. De tal manera que:

> […] serían incompatibles con la Convención Americana las restricciones sustantivas definidas en disposiciones administrativas o las regulaciones amplias o ambiguas que no generan certeza sobre el ámbito del derecho protegido y cuya interpretación puede dar lugar a decisiones arbitrarias que comprometan de forma ilegítima los derechos a la intimidad y a la libertad de expresión. (815) [931]

En el caso Paraguay, la Relatoría determina que este país "no cuenta con una legislación especializada sobre protección de los datos personales que disponga de resguardos suficientes –incluida la supervisión de órgano autónomo y especializado– frente al posible abuso del control que tienen los agentes tanto públicos como privados sobre los datos personales sensibles." (1022) [932] De esta manera, la Relatoría Especial se mantiene en la recomendación previa que señaló que para garantizar la vigencia de este derecho era indispensable la existencia de una ley, de un órgano que viabilice su aplicación y de la necesidad de que éste sea independiente no solo porque controlará a particulares sino a instituciones públicas. Aclarándose que, estos datos pueden o no ser sensibles pues como vimos en repetidas ocasiones es suficiente con que sean de carácter personal para que la protección prospere. Esta sin duda es una de las cuestiones que aún debe pulirse respecto del contenido del derecho a la privacidad y su fundamental diferencia con el derecho a la protección de datos personales.

[925] *Ibíd.*
[926] *Ibíd.*
[927] *Ibíd.*
[928] *Ibíd.*
[929] *Ibíd.*
[930] *Ibíd.*
[931] *Ibíd.*
[932] *Ibíd.*

Asimismo, respecto de trasparencia indica que "las leyes deben asegurar que el público pueda acceder a información sobre el alcance, uso y controles existentes para garantizar que este tipo de programas no puedan ser usados de manera arbitraria" (1022)[933]. Asimismo, ha recomendado que:

> […] los intermediarios deberían tener la protección suficiente para hacer públicas las solicitudes realizadas por agencias del Estado, u otros actores legalmente facultados, que interfieran con el derecho a la libertad de expresión o la privacidad de los usuarios. Es una buena práctica, en este sentido, que las empresas publiquen de manera regular informes de transparencia en los que revelen cuando menos, el número y el tipo de las solicitudes que pueden aparejar restricciones al derecho a la libertad de expresión y a la privacidad de los usuarios" (1022). [934]

Además, la Relatoría Especial reitera lo señalado en el informe sobre el derecho a la privacidad en la era digital de 2014, en el que la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos señaló que:

> […] los metadatos de las comunicaciones digitales, que incluyen, entre otros, la ubicación, actividades en línea, y con quiénes se comunican los usuarios de Internet, pueden ser altamente reveladores, y su recolección y conservación equivalen a una limitación directa al derecho a la intimidad y vida privada de las personas (…) [l]a agregación de la información comúnmente conocida como 'metadatos' puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada. (1024)[935]

Esta afirmación es sustancial porque dimensiona a la acumulación masiva de datos personales como un mecanismo aún más invasivo que la interceptación de comunicaciones. Y en este sentido, lo mismos criterios revisados anteriormente y que limitan este mecanismo deben cumplirse para verificar que su uso no sea contrario a los derechos humanos.

En el caso de El Salvador, la Relatoría Especial ha considerado fundamental que los Estados protejan el derecho a la libertad de expresión y acceso a la información en Internet, para lo cual es necesario garantizar:

> […] la privacidad de las comunicaciones digitales, así como la confidencialidad, integralidad y disponibilidad de los datos y sistemas informáticos. La adopción de marcos legislativos para prevenir y sancionar la delincuencia cibernética y la realización de conductas punibles a través de medios informáticos es una medida importante para lograr esos objetivos. (757)[936]

La ciberseguridad es entonces un elemento sustancial para garantizar la privacidad, ya que solo a través de mecanismos tecnológicos que garanticen la disponibilidad, seguridad y confidencialidad de los canales de comunicación y la forma de almacenaje de esta, se puede evitar el uso ilícito de datos personales con los que se intenta perjudicar a sus titulares.

---

[933] *Ibíd.*
[934] *Ibíd.*
[935] *Ibíd.*
[936] *Ibíd.*

En cuanto a Honduras, la CIDH advierte que la Ley de 2011 que existen indeterminaciones en la ley que establece la obligación de las empresas o instituciones a retener, de cada usuario, por el plazo de 5 años, sus "números de teléfono conectados, duración y hora de la llamada y, en el caso de teléfonos móviles, la ubicación desde donde se realiza la llamada, contesta, o envía un mensaje" (851). [937]

Esto porque, dicha normativa no aclara quienes serán los sujetos obligados, ya que no se distingue si se trata de proveedores de servicios de internet incluyendo a los de servicio como plataformas de correo electrónico, redes sociales, servicios de mensajería, entre otras. Pero además, porque tampoco determina que tipos de delito autorizan esta retención de datos (853). Señalando que los plazos de retención son los más extenso y onerosos en la región y que además no se dispone la destrucción de los datos conservados al finalizar el plazo de retención. Finalmente, la Relatoría determina como errónea la "práctica de vigilancia histórica – en contraposición a mecanismos de retención selectivos y limitados claramente por ley". [938] En este sentido, los datos personales solo deben retenerse con fines de orden público o de seguridad de forma limitada y selectiva, para lo cual deben aplicarse criterios legales y judiciales que garanticen un equilibrio y ponderación de derechos.

Finalmente, como hemos visto, las tecnologías basadas en datos pueden destinarse a usos beneficiosos, estos avances tecnológicos plantean riesgos para la dignidad humana, la autonomía, la vida privada y el ejercicio de los derechos humanos. Por ello, el Consejo de Derechos Humanos creó el mandato del Relator Especial sobre el derecho a la privacidad en julio de 2015[939]. Ahora bien, en dicho informe se menciona a la privacidad como derecho sustancial que debe ser reportado a través de esta relatoría y no al derecho a la protección de datos personales, postura que debe ser superada para que el trabajo de este organismo sea completo, ya que necesita evaluar y trabajar en pro de la protección completa de la dignidad humana en entornos digitales.

Ya que, como hemos podido analizar de las distintas recomendaciones que la Relatoría Especial ha realizado a los países citados, existe un estrecho vínculo entre privacidad, protección de datos personales, libertad de expresión y transparencia. Pero además, se han incluido como elementos del derecho a la privacidad, aquellos criterios de manejo adecuado de datos personales. En este sentido, se está ampliando la visión original de este derecho para incluir en él condiciones y elementos propios del derecho a la protección de datos personales.

2.1.19 Informe 2016

[937] *Ibíd.*
[938] *Ibíd.*
[939] Asamblea General de las Naciones Unidas, Resolución 28/16 sobre el derecho a la privacidad en la era digital, 1 de abril de 2015, accedido el 14 de septiembre de 2019, Resolución https://www.google.com/search?q=resoluci%C3%B3n+del+Consejo+de+Derechos+Humanos+28%2F16&oq=resoluci%C3%B3n+del+Consejo+de+Derechos+Humanos+28%2F16&aqs=chrome..69i57j33l2.982j0j7&sourceid=chrome&ie=UTF-8

Para el año 2016, 33 periodistas y trabajadores de medios de comunicación social fueron asesinados[940], lo que evidencia la crisis que enfrenta el derecho de libertad de expresión en el hemisferio.

El citado informe realiza un análisis por países miembros de la OEA. A continuación se detallan, únicamente, aquellas recomendaciones relativas a datos personales o privacidad.

El caso colombiano, determina la necesidad de que los programas de vigilancia sean "diseñados e implementados atendiendo a los estándares internacionales en materia de derechos humanos"[941], en especial que las definiciones sobre privacidad, espacio público o los ámbitos que integran el sistema de vigilancia no sean indeterminados o demasiado amplios que puedan ser interpretadas de manera arbitraria. (383) Debido a que las autoridades necesitan un ámbito de regulación específico que determine condiciones, causas y características de aplicación para limitar la ejecución de esta práctica.

En cuanto a Estados Unidos, por pedido de su unidad de Inteligencia, la compañía *Yahoo* habría accedido a millones de correos electrónicos de sus clientes y a escanearlos buscando información específica. El Relator Especial para la Libertad de Opinión y Expresión de Naciones Unidas, David Kaye, manifestó que esta forma de búsqueda de información no cumple con estándares de necesidad y proporcionalidad para la protección de intereses legítimos del gobierno, procedimientos que por el contrario podrían afectar la libertad de expresión. (637) Y es que la vigilancia masiva de correos es una acción desproporcionada que afecta la privacidad de aquellas personas que no tienen relación alguna con algún categoría sospechosa que justifica la intervención de una autoridad de control.

Por su parte, la Suprema Corte de Justicia de México, en resolución de 4 de mayo, declaró constitucional los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión por las cuales:

> […] se obliga a los concesionarios de telecomunicaciones a conservar durante dos años el registro de las comunicaciones realizadas y los metadatos que permitan identificar al usuario el tipo de comunicación, información relacionada con los servicios de comunicación utilizados, así como información sobre la geolocalización en tiempo real de teléfonos móviles (878) […] y a entregarla a las autoridades competentes, de acuerdo con el procedimiento legal establecido para ello (879) […] La Corte concluyó que la geolocalización en tiempo real de teléfonos móviles, no constituye una intervención en las comunicaciones por lo que se puede llevar a cabo sin orden judicial.[942]

Esta última aseveración realizada por la Corte resulta problemática debido a que la geolocalización puede resultar útil para la provisión y mejoramiento de bienes y servicios. Sin embargo, si los datos de geolocalización se usan de forma indebida puede significar un grave atentado a las libertades individuales como el derecho al libre tránsito, a la libre reunión, entre otros. No solo debe analizarse este tema desde la perspectiva de privacidad sino desde los principios y derechos propios de la protección

[940] *Ibíd.*
[941] *Ibíd.*
[942] *Ibíd.*

de datos personales que precautelan un almacenamiento masivo, injustificado y desproporcionado.

De otro lado, el Perú y Trinidad y Tobago también fueron observados por la Relatoría Especial. Para el diseño e implementación de tareas de vigilancia es necesario que, en el marco de un debido proceso, se dicten órdenes judiciales públicas, en las que se analice la proporcionalidad de la petición, respecto del interés general que se quiere promover o proteger.

En cuanto a Chile, se recomienda al Estado que se legisle sobre temas:

> […] identificados como esenciales para el respeto de los derechos en Internet, tales como la neutralidad de la red, los límites y controles a la vigilancia estatal y privada en Internet y las salvaguardas para el ejercicio de la libertad de expresión y privacidad en las políticas de ciberseguridad (1282).[943]

La postura de la Relatoría Especial, evidencia los mecanismos mínimos que los Estados deben cumplir para proteger a las personas en los entornos digitales. No es suficiente que la privacidad esté recogida en políticas de ciberseguridad. Porque no se trata de un enfoque de seguridad de los datos personales sino de un sistema integral de protección que determine: principios, derechos y obligaciones.

De otro lado, esta Relatoría actualiza el informe 2013 sobre Estándares para una Internet Libre, Abierta e Incluyente. Para lo cual, incluye los estándares, principios rectores y relativos a privacidad, desarrollados por la CIDH y su Relatoría Especial.

Dicho informe hace referencia a la privacidad y no a la protección de datos personales pues señala que:

> Con el advenimiento de internet surgieron numerosos desafíos en torno a la protección del derecho a la privacidad, tanto para el Estado, en su rol de garante, como para los particulares, en su rol de usuarios. (…) El impacto de la tecnología sobre la privacidad se hizo evidente con la introducción de los medios de comunicación y las fotografías de circulación masiva. (…) Con internet, la capacidad técnica para reunir, almacenar e intercambiar información personal que brindan las tecnologías digitales generó un nuevo desafío en la protección de la privacidad. [944]

Ahora bien, del texto dispuesto resulta valiosa la apreciación de que, también los actores privados tienen la responsabilidad de respetar los derechos humanos en línea. Pues les establece responsabilidades; no solo tienen la obligación, desde una postura negativa, de abstenerse de restringir derechos; sino que, aún más importante, tienen un deber positivo de crear un entorno en el que se respeten los derechos, a través de la generación de evaluaciones de impacto y sistemas de denuncias accesibles y eficaces. Todo ello con la finalidad de identificar daños reales o potenciales a los derechos humanos causados por sus servicios o actividades.[945]

Asimismo, en dicho informe constan los principales hitos que la Relatoría Especial ha señalado sobre privacidad:

---

[943] *Ibíd.*
[944] *Ibíd.*
[945] *Ibíd.*

a) Los Estados tienen la obligación de respetar y proteger el derecho a la privacidad en la era digital y adoptar o adaptar su legislación y sus prácticas al efecto, protegiendo a todas las personas bajo su jurisdicción, lo que incluye la protección frente a posibles injerencias arbitrarias o abusivas también respecto de terceros.
b) El *habeas data* sigue siendo considerada una garantía para el acceso a la información personal, su actualización, rectificación o eliminación; y además, para la transparencia de los actos de gobierno. En los países que reconocen el derecho a la protección de datos personales, el *habeas data* se convierte en un medio para la efectivización del derecho. En el caso de Ecuador, por carecer de normativa legal que desarrolle un sistema preventivo, únicamente existe un sistema reactivo a través de esta garantía constitucional.
c) La protección de los datos personales constituye un fin legítimo para establecer restricciones al derecho a la libertad de expresión, no obstante, cualquier limitación al derecho a la libertad de expresión -sea para proteger la privacidad, como en el caso de los datos personales, la honra o reputación-, debe respetar el test tripartito desarrollado por la jurisprudencia y doctrina interamericana: estar legalmente establecido en una ley en sentido formal y material, ser necesaria e idónea, y proporcional.[946] Los ordenamientos jurídicos tampoco pueden contener sanciones penales para proteger estos derechos.
d) Si bien la protección de datos personales constituye un objetivo legítimo, en ningún momento puede ser invocada para limitar o restringir la circulación de información de interés público, sobre funcionarios o personas públicas, o candidatos en el ejercicio de sus funciones, o que involucran violaciones de derechos humanos.
e) La protección de la privacidad en internet requiere que se garantice la confidencialidad de los datos personales en línea.
f) El hecho de que la persona voluntariamente deje rastros públicos de sus actividades en *blogs* o redes sociales no habilita al Estado a recolectar esta información masiva ni sistemática salvo en las circunstancias específicas donde "dicha injerencia estuviera justificada"[947], pues hacerlo constituye una injerencia en la vida privada de las personas. (214)

Así como ocurrió en Europa, la OEA y las Relatorías Especiales han comenzado a incorporar análisis y referencias a la protección de datos personales. Aun no se lo hace desde la perspectiva de reconocerlo como un derecho autónomo sino desde la perspectiva de otorgar a la privacidad elementos adicionales que lo transformen en un derecho abarcador.

Las principales referencias que dicho informe tiene sobre datos personales y que demuestran la línea de pensamiento de la Relatoría Especial y su Comisión, respecto de su importancia para la garantía de derechos humanos en línea, son las siguientes:

a) El derecho a la privacidad en internet, "requiere que se garantice la protección en el tratamiento de los datos personales en línea". (204)[948]

[946] *Ibíd.*
[947] *Ibíd.*
[948] *Ibíd.*

b) En América Latina en general se ha adoptado una noción amplia de datos personales que "incluye cualquier dato propio de personas físicas o jurídicas, identificadas o identificables". (204)[949]
c) Los datos personales sensibles son aquellos que se refieren al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral y familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, la propia imagen, la intimidad personal y familiar, o el entorno laboral de una persona.[950]
d) Los datos biométricos que son aquellos que permiten "el reconocimiento sistemático de individuos basado en sus características conductuales y biológicas"[951] (209) requieren un tratamiento estricto basado en el respeto a los derechos humanos y en criterios de necesidad y proporcionalidad, sobre todo al momento de la determinación del tipo de datos y los métodos de recolección. Así mismo, cuando son recolectados por el Estado, exigen un alto nivel de transparencia, en cuanto a su finalidad y uso y además de controles administrativos y judiciales. (209)
e) Debido a la naturaleza transfronteriza de internet, la necesidad de regular el tratamiento de datos no se limita al ámbito nacional sino que implica la necesidad de desarrollar un marco normativo internacional.[952]
f) Resulta fundamental que se desarrollen regímenes de protección de datos que regulen el almacenamiento, procesamiento, uso y transferencia de datos personales ya sea tanto entre entidades estatales como respecto de terceros. (204)[953]
g) Los Estados deben adoptar políticas tendientes a prohibir el tratamiento de datos personales, incluido el almacenamiento, análisis, y divulgación salvo cuando estén legitimados para hacerlo o exista consentimiento informado de la persona afectada. El consentimiento de la persona habilita a los Estados y particulares al tratamiento de sus datos personales.[954]
h) Debe prohibirse el uso de datos personales para fines contrarios a los derechos humanos y establecerse mecanismos de supervisión efectivos e independientes. (205)[955]
i) El Estado o quien haga el tratamiento de datos debe establecer pautas y controles necesarios para verificar 1) que los datos no se utilicen para fines distintos a los denunciados, 2) que el mantenimiento y almacenamiento de datos se haga conforme a dichos fines y solo durante el plazo informado y consentido, y 3) que los datos sean compartidos o difundidos sólo en las condiciones y para los fines consentidos e informados. (206)[956]
j) Se deben adoptar medidas positivas tendientes a educar a las personas en torno a sus derechos y las condiciones legales para el tratamiento de datos personales, informando cuando hubiera recolección, almacenamiento, tratamiento o divulgación de datos. (205)[957]

[949] *Ibíd.*
[950] *Ibíd.*
[951] *Ibíd.*
[952] *Ibíd.*
[953] *Ibíd.*
[954] *Ibíd.*
[955] *Ibíd.*
[956] *Ibíd.*
[957] *Ibíd.*

k) Tanto a nivel regional como universal se reconoce que las prácticas de vigilancia y la intercepción y recopilación ilícita o arbitraria de datos personales no sólo afectan el derecho a la privacidad y a la libertad de expresión sino que también pueden ser contrarios a los preceptos de una sociedad democrática. (207)[958]

l) El aparecimiento de nuevas formas de uso, almacenamiento, procesamiento y difusión afectan la privacidad y la protección de los datos personales, tales como:
    a. El modelo de negocio gratuito de las redes sociales en el que los datos de sus usuarios se venden a terceros. (199)
    b. El cruce entre IP y GPS que afecta directamente a la privacidad pues permite localizar y rastrear datos personales e incluso físicamente a los titulares de los dispositivos. (200)
    c. Las herramientas de extracción de información personal y de rastreo de la actividad de los usuarios de internet como: *cookies y los web bugs*. (201)

m) Los cinco principales desafíos generados o magnificados por el fenómeno de internet: a) la protección de datos personales; b) la vigilancia, monitoreo e interceptación; c) la encriptación y el anonimato; d) "*Big Data*" y e) Internet de las Cosas. (202)

n) El anonimato constituye un medio para la protección de la privacidad pues permite la libertad de expresión al facilitar la participación en el discurso público sin identificarse, evitando de esta manera posibles represalias asociadas con la opinión. Sin embargo, el anonimato puede levantarse cuando los discursos no estén amparados por el derecho a la libertad de expresión como: la propaganda en favor de la guerra, la apología del odio, la violencia, al genocidio, la pornografía infantil. Asimismo, cuando se hubieren determinado responsabilidades ulteriores de forma legítima. (229) [959]

o) Los Estados pueden "tomar medidas para identificar fehacientemente a una persona en el marco de una investigación judicial y siempre que se respete el marco de proporcionalidad". [960] (229)

p) La encriptación es un mecanismo que coadyuva a la privacidad, ya que, a través de la codificación de datos en tránsito y remotos, solo los destinatarios deseados puedan acceder a estos. Por ello, los Estados no deben restringir de manera general o por defecto, salvo en casos legales, necesarios y proporcionales, la encriptación como mecanismo para protegerse de las invasiones ilegítimas a la privacidad. (230) Así como tampoco se debe permitir "la imposición de registros de claves centralizados, o la creación de puertas traseras –*back doors*- para habilitar la interceptación de comunicaciones incluso en aparatos encriptados"[961]. (231)

q) La captura, almacenamiento, análisis y sistematización en busca de tendencias y perfiles, a través de tecnologías como el *Big Data*, también plantean desafíos para la privacidad. El *Big Data* puede ser útil para el diseño de políticas públicas que mejoren el desempeño estatal, así como para mejorar bienes y servicios privados. (232) Sin embargo, existen problemas de regulación en torno a la propiedad y el traspaso de los datos, pero también en torno a las tecnologías disponibles para el análisis. Ya que, muchas de estas no permiten el análisis

[958] *Ibíd.*
[959] *Ibíd.*
[960] *Ibíd.*
[961] *Ibíd.*

"objetivo de datos y tendencias, sino que inescindiblemente permiten la identificación de los usuarios" [962] que conforman la masa crítica analizada. (233)

r) El Internet de las Cosas también presenta un reto para la protección de datos y la privacidad, ya que los *chips* electrónicos incorporados a productos cotidianos, con un identificador individual único, que pueden comunicarse y recopilar información y trasmitirla a las empresas proveedoras de servicios sin que el titular conozca de esta "red de información continua que conecta a los objetos en las vidas de las personas" pudiera afectar a los derechos humanos en línea. (234)

s) Respecto de regiones de alta peligrosidad para ejercer la libertad de expresión, la Relatoría Especial ha dictado un informe titulado "Cómo desarrollar la seguridad digital para el periodismo". En el cual, se identifican varias tecnologías que permiten establecer salvaguardas no solo aplicables a los contenidos, sino también a los medios que los transmiten: "desde las aplicaciones que se utilizan para encontrar información, hasta los códigos y protocolos que conectan los dispositivos con el mundo digital, y el propio hardware, los cables y torres inalámbricas que transportan datos". [963] (235)

t) Toda vigilancia masiva de comunicaciones y datos supone la interceptación de la red, de cables, equipos o datos de intermediarios o terceros (210), y por lo tanto, la vigilancia en todas sus modalidades constituye una injerencia en la vida privada. Como ha señalado la Relatoría Especial en informes previos las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas deben ser autorizadas por autoridades judiciales independientes, que deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que persigue en el caso concreto; si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario y si resulta proporcional respecto del interés que se quiere promover.

Los estándares desarrollados tanto en el sistema interamericano como en el europeo apuntan a la protección no solo del contenido de las comunicaciones sino también a los datos respecto de esas comunicaciones, y en el caso de internet, de los metadatos (213).

Finalmente, sobre la legitimidad del derecho al olvido, es decir de las medidas de remoción y desindexación de contenidos en línea y la adecuada ponderación de los límites entre el derecho a la privacidad y el derecho a la libertad de expresión e información en Internet. El 2014, Tribunal de Justicia de la Unión Europea en el caso "Google Spain S.L., Google Inc. vs. Agencia Española de Protección de Datos, Mario Costeja González", determinó que:

> […] los buscadores - intermediarios que indexan contenidos alojados en otras plataformas – Google, Yahoo, Bing, etc.- hacen tratamiento de datos personales, en tanto controladores de datos, y en ese entendido, de acuerdo a la Directiva Europea N. 95/46/CE, las personas pueden ejercer el derecho a cancelar el tratamiento de datos cuando hubiere motivos que lo justifiquen. (…) las personas pueden solicitar que sus datos personales sean desindexados de los motores de búsqueda de Internet, amparándose en la protección de los datos personales en internet. (128) [964]

[962] *Ibíd.*
[963] *Ibíd.*
[964] Sentencia de la Gran Sala del tribunal de Justicia de la Unión Europea, 13 de mayo de 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, accedido el 19/10/2019 en https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

Dicha resolución plantea que, para que opere este derecho se requieren una serie de condiciones descritas a continuación:

a) la indexación de información debe referirse a una persona física;
b) la información relativa a esta persona afecta potencialmente a una multitud de aspectos de su vida privada y puede establecer un perfil sesgado o equivocado;
c) La decisión no elimina ni modifica la información del sitio que aloja o genera la información original;
d) la información personal es "inadecuada, irrelevante o ya no es relevante o es excesiva"[965];
e) la información personal no reviste interés público.

Por su parte, la Relatoría Especial sostiene que el reconocimiento de este derecho tiene falencias que se describen a continuación:

a) los conceptos centrales para la evaluación de los intereses en juego no fueron desarrollados con mayor detalle por el Tribunal, lo que ha dado lugar a una serie de interpretaciones vagas o ambiguas en distintas jurisdicciones.[966]
b) Se delegó al sector privado la obligación de recibir, analizar y decidir sobre las solicitudes de desindexación.
c) En América Latina, se han registrado solicitudes de remoción de contenidos y no solo de su desindexación, a periódicos, blogs y periodistas.[967]
d) Organizaciones de la sociedad civil también han denunciado que funcionarios públicos de diversos países estarían utilizando el derecho al olvido para cancelar información de interés público, instaurando en muchos casos la práctica de reemplazar acciones de calumnias e injurias ante los tribunales por acciones de oposición ante la autoridad de protección de datos personales. (968) La CIDH y la Corte Interamericana ha afirmado reiteradamente que los funcionarios públicos están sujetos a un mayor escrutinio por parte de la sociedad, y por ello, "debe existir una fuerte presunción en contra de solicitudes de desindexación y/o cancelación de información presentadas por funcionarios públicos, personas públicas, o candidatos a ejercer cargos públicos". [969] (137)

Estas prácticas y problemáticas descritas han motivado a la Relatoría Especial por la libertad de expresión a tomar la siguiente postura:

> […] la remoción de contenidos en internet tiene un impacto evidente en el derecho a la libertad de expresión, tanto en su dimensión individual como social, y en el derecho de acceso a la información por parte del público. La información removida no circula, lo que afecta el derecho de las personas a expresarse y difundir sus opiniones e ideas y el derecho de la comunidad a recibir informaciones e ideas de toda índole. Un efecto similar, aunque no exactamente igual por su dimensión, es el que produce la desindexación de contenidos, en tanto los mismos se hacen más difíciles de encontrar y

[965] *Ibíd.*
[966] OEA, "Informes Anuales, OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo", 2009, accedido 20 de noviembre de 2017, http://www.oas.org/es/cidh/expresion/informes/anuales.asp.
[967] *Ibíd.*
[968] *Ibíd.*
[969] *Ibíd.*

> se invisibilizan. Ambos tienen un efecto limitador en la libertad de expresión en tanto restringen la posibilidad de buscar, recibir y difundir informaciones e ideas por parte de todas las personas, sin consideración de fronteras nacionales.[970]

Al respecto, las democracias latinoamericanas son débiles respecto del acceso y transparencia a la información pública y militar como mecanismo para el ejercicio a la libertad de expresión. Por ello es que incluso se ha señalado que respecto de graves violaciones de los derechos humanos, la población quiere y debe recordar y no olvidar.[971]

La Relatoría Especial señala la necesidad de distinguir entre información y datos personales, como criterio que limite la eliminación de noticias de prensa que afecten la libertad de expresión, sobre todo cuando el medio de comunicación usa internet como plataforma. (137) Pues como regla general, que incluso se incorpora en las diversas legislaciones nacionales sobre protección de datos, el contenido generado por un medio de comunicación no está sujeto a protecciones derivadas del derecho de *habeas data* (138).[972] Este análisis determina que:

> […] las plataformas digitales de los medios informativos no son controladores de datos personales, sino fuentes públicas de información y plataforma para la transmisión de opiniones e ideas sobre temas de interés público, y como tal no pueden ser susceptibles de una orden de desindexación, ni tampoco la supresión de un contenido en línea de interés público. (138) [973]

En el mismo sentido, la Relatoría Especial establece que el derecho al olvido no procede ante la "difusión de noticias falsas agraviantes o inexactas en medios digitales".[974] Puesto que respecto de las publicaciones periodísticas, existen mecanismos como la rectificación y la réplica, e incluso otros de índole civil que buscan indemnización por daños y perjuicios. El derecho a la libertad de expresión, como ha señalado repetidamente la Relatoría establece un sistema de responsabilidad posterior, por ser el menos lesivo. Puesto que, la censura previa, que sería un sistema preventivo, afectaría directamente a la libertad de expresión. Además, un sistema de responsabilidad post permite establecer que quien demanda soporte "la carga de la prueba de la falsedad o inexactitud de la información divulgada"[975]. (139)

Por lo que, esta postura de la Relatoría Especial debe ser escuchada por los países latinoamericanos que deberán evaluar sus realidad sociales para decidir sobre la incorporación o no, en su ordenamiento jurídico, del denominado derecho al olvido. Tomando en cuenta que la desindexación o cancelación de la información podría impedir el acceso a asuntos de interés público; y afectaría la expresión lícita y legítima.

Sin embargo, si un país decide incluir al olvido como derecho, es necesario establecerlo como régimen absolutamente excepcional, con un catálogo estricto, claro y limitado sobre la procedibilidad de la desindexación para que su aplicación no afecte el derecho a la verdad y a la memoria, (137) Asimismo, debe establecer mecanismos de

[970] *Ibíd.*
[971] *Ibíd.*
[972] *Ibíd.*
[973] *Ibíd.*
[974] *Ibíd.*
[975] *Ibíd.*

transparencia en su aplicación como una publicación regular "sobre la naturaleza, el volumen y los resultados de las solicitudes de desindexación".[976] (218) Además, no podría usarse como mecanismo preventivo o cautelar para proteger el honor o la reputación. Ya que sobre estos derechos existen otros procedimientos que buscan indemnizaciones y reparaciones. El derecho al olvido debería limitarse únicamente a:

> […] aquellos casos en que el solicitante demuestre un daño sustantivo a la privacidad y la dignidad y siempre a través de una orden judicial adoptada en el marco de un proceso respetuoso del debido proceso y en el que puedan ejercer su defensa todas las partes involucradas, incluyendo quien se expresa, el medio de comunicación o editor del sitio web que pudiera verse afectado y los intermediarios. De este modo se evita que sean las empresas privadas que operan los buscadores y otras plataformas a quienes les corresponda analizar y decidir sobre la pertinencia de restringir el acceso a contenidos en línea bajo estos supuestos. (140).[977]

De lo anteriormente analizado se concluye que, "tanto para el Estado, en su rol de garante, como para los particulares, en su rol de usuarios"[978], el internet y las nuevas tecnologías presentan numerosos retos para la vigencia y aplicabilidad de los derechos humanos, en especial de la privacidad.

Pero en esta nueva realidad, no solo las transgresiones aparecen sino varios nuevos derechos fundamentales que van más allá de la protección a la libertad de expresión o a la privacidad y que enmarcan nuevas formas de proteger la dignidad humana de las personas en entornos digitales.

Prueba de ello es el aparecimiento del concepto de ciberseguridad, por el cual, se protege "la privacidad de las comunicaciones digitales, así como la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos"[979]. Es decir, las personas pueden favorecerse de los beneficios del uso de los medios tecnológicos y los Estados tienen la obligación de proporcionarles medios ciberseguros no solo para favorecer otros derechos como la privacidad o la libertad de expresión sino como elemento indispensable, que debe ser reconocido como tal, para que un individuo pueda desarrollarse libre y plenamente en entornos digitales.

Asimismo, se colige una paulatina transformación de la protección de datos de un problema de captura, análisis y uso general de la información personal, sobre todo respecto de la regulación en torno a la propiedad y el traspaso de los datos, en un reconocimiento de la titularidad del dato personal. Es decir, un reconocimiento por el cual, el dato soy yo. Esto es, la virtualización de la persona real, dado que lo que pasa en línea afecta a la persona fuera *off line*.

Se debe entonces propender a que los Estados, independientemente del modelo de protección que adopten, procuren tanto en el ámbito público como en el privado utilizar tecnologías como el *big data*, el internet de las cosas, las *cookies, los bugs*, entre otras, de manera adecuada, legal y proporcional. Pues la recolección y tratamiento masivo y esquematizado de datos personales debe respetar los derechos humanos, ser

[976] *Ibíd.*
[977] *Ibíd.*
[978] *Ibíd.*
[979] *Ibíd.*

excepcional, transparente y controlado por entidades administrativas y judiciales como garantía de que efectivamente la finalidad y uso sea el correcto.

Asimismo, los Estados deben evitar la implementación de leyes, políticas y usos que prohíban de manera generalizada el cifrado, el anonimato como mecanismos que permiten proteger la privacidad de los titulares. Asimismo, deben establecer limitaciones, únicamente, si estas con necesarias, proporcionales, legítimas y permitan la asignación de responsabilidades ulteriores a través de un proceso judicial en el que se cumpla con el debido proceso.

2.1.20 Informe 2017[980]

Este informe plantea nuevos desafíos a la libertad de expresión derivados del aumento de la vigilancia indirecta o masiva y de las prácticas de retención de datos personales, con el fin de mantener el orden público y por motivos de seguridad.

La Relatoría Especial del 2017 nuevamente considera que la privacidad debe ser un principio orientador del entorno digital, un presupuesto del ejercicio del derecho a la libertad de expresión en línea que debe ser protegido por la ley y estrictamente promovido en la política pública. [981]

Para la Relatoría, el concepto de privacidad es inherente al de la intimidad y como tal está garantizado en los principales instrumentos interamericanos y universales de derechos humanos. De ahí que el tendiente avance tecnológico se debe incorporar el derecho a la protección de datos personales dentro del ordenamiento constitucional y el desarrollo de normativa de los países.

En esta relatoría, se reconoce el *estatus* de algunos países de América Latina y del Caribe que han trabajado en procesos de construcción de una normativa que regule la información personal de los ciudadanos, recociendo además los procesos para este fin.

En el caso Argentina, se cuestiona el Decreto de Necesidad y Urgencia 746/2017, que modifica las disposiciones de la ley 27.275 y establece que la Agencia de Acceso a la Información Pública, como la Autoridad encargada de la Aplicación de la Ley de Protección de Datos Personales N° 25.326. Para la Relatoría este cambio no garantiza que un órgano de control independiente de posibles injerencias del Ejecutivo, sea el encargado de la protección de datos personales, puesto que su autonomía funcional se encontraría cuestionada debido a que para su estructura institucional se requiere de la aprobación del Jefe de Gabinete. Adicionalmente, se plantean dudas sobre:

> […] la concentración en un único organismo de las funciones de acceso a la información pública y de protección de datos personales, por considerarlas derechos de la misma jerarquía que reflejan similares capacidades institucionales para ejercer su función.[982]

[980] Ibíd.
[981] *Ibíd.*
[982] *Ibíd.*

Este modelo hibrido también existe en México. Lo importante es garantizar que cada una de las funciones y atribuciones se encuentren debidamente institucionalizadas, de tal manera que, incluso las autoridades de una y otra competencia se encuentren plenamente diferenciadas y puedan ejercer sus competencias desde las propias perspectivas de cada uno de los derechos para evitar confusiones e imparcialidades.

En Bahamas, se establece que ciertos registros no podrán ser divulgados por considerarlos datos personales confidenciales. Esta decisión estará sujeta a revisión, para lo cual se nombrará un administrador de información, que resolverá sobre las posibles denuncias de protección. Así como, se encargará de la publicación de un código sobre normas mínimas y de mejores prácticas.

En cuanto al caso Ecuador, la Relatoría realiza el análisis de la denuncia de los hechos producidos durante la administración del expresidente Rafael Correa, quien, el 19 de junio de 2017, convocó a sus seguidores de la red social Twitter, para que, a través de esta red social, averigüen y expongan la identidad y datos personales de quienes lo insultan y critican. (459) De esta forma, pretendía atacar a quienes eran abiertamente oposición o no estaban de acuerdo con el régimen.

Esta postura provocó una marcada confrontación, a través de descalificaciones y estigmatizaciones constantes. Se generó un clima de represión que limitó la exposición de asuntos públicos. Destaca de singular manera las relaciones tensas entre la prensa y el gobierno, lo que polarizó de los espacios para debates y generó opiniones sesgadas. (460)

Además, la Relatoría Especial indicó que se reportaron varios casos de limitaciones a la libertad de expresión en Internet, como la suspensión o el bloqueo de cuentas de la red social Twitter tras publicaciones de contenido político o sobre actualidad, un fenómeno que preocupa a las organizaciones de la sociedad civil y que llama la atención a las empresas de Internet por la reiteración de este fenómeno en Ecuador. La Relatoría recomendó que las máximas autoridades del Estado tengan entre sus deberes el "de contribuir a generar un clima de mayor tolerancia y respeto por las ideas ajenas, incluso cuando las mismas le resulten ofensivas o perturbadoras". (460)[983] Aún más, la Relatoría Especial recuerda que:

> […] los funcionarios públicos tienen el deber de asegurarse que con sus pronunciamientos no están lesionando los derechos de quienes contribuyen a la deliberación pública mediante la expresión y difusión de su pensamiento, tales como periodistas, medios de comunicación y organizaciones defensoras de derechos humanos y deben atender al contexto en el cual se expresan para asegurarse que sus expresiones no constituyan, en palabras de la Corte, "formas de injerencia directa o indirecta o presión lesiva en los derechos de quienes pretenden contribuir a la deliberación pública mediante la expresión y difusión de su pensamiento" [984].

Y es que las autoridades públicas, conforme han señalado en varias resoluciones de la CIDH y la propia Relatoría, por su propia voluntad han accedido a funciones públicas y en consecuencia deben aceptar con humildad el escrutinio público y las críticas de sus mandantes, reflexionar sobre las observaciones y comentarios, verificar si se encuentran o no justificadas, todo ello en garantía de una auténtica democracia participativa.

[983] *Ibíd.*
[984] *Ibíd.*

En otro caso, Cedatos, encuestadora que emitió resultados sobre una "boca de urna divulgados tras las elecciones del 2 de abril, que eran favorables al candidato de la oposición Guillermo Lasso"[985] denunció haber sido víctima de interceptación ilegal de información y violación de la privacidad de sus correos electrónicos, por lo que presentó denuncia ante la Fiscalía.

En este contexto, la Relatoría recomienda que las decisiones de realizar tareas de vigilancia, su legalidad, las tecnologías utilizadas y su impacto en el ámbito de los derechos deben estar autorizadas por autoridades judiciales especializadas e independientes, a través de procesos en los que se garantice el debido proceso. Estas resoluciones deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que se persigue en el caso concreto.

En cuanto a Chile, la Relatoría reconoce el esfuerzo de Chile de mejorar su estándar de protección cuanto, la presidenta Michelle Bachelet, el 13 de marzo de 2018, firmó el Proyecto de Ley que Regula la Protección y el Tratamiento de los Datos Personales, que busca modificar la Ley Nº 19.628 sobre Protección de la Vida Privada. Esta iniciativa busca cumplir con los estándares internacionales en materia de tratamiento de datos personales y además acogerse a las directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE). Además, establece un amplio catálogo de derechos que le asisten al titular de los datos y crea la Agencia de Protección de Datos Personales.

Sobre Colombia y El Salvador, la Relatoría Especial recuerda que los Estados deben garantizar que la interceptación, la recopilación y el uso de la información personal estén claramente autorizados por la ley a fin de proteger a las personas de la interferencia arbitraria o abusiva de su privacidad. Adicionalmente, que los procesos de investigación que se lleven adelante y que impliquen una invasión de la privacidad deben ordenados por un juez competente que respete el debido proceso.

Sobre el caso Estados Unidos, la Relatoría Especial considera que las declaraciones y ataques del Presidente Trump, contra medios de comunicación acusándolos de opositores y de parcialidad política, en apariciones públicas y a través de redes sociales:

> […] son particularmente graves, en tanto pueden agravar el riesgo de amenazas y violencia contra periodistas en el país y erosionar la confianza que tiene la población en el periodismo como institución de la democracia. Asimismo, la actual administración emitió diversas amenazas directas de posibles acciones gubernamentales o procedimientos legales contra medios de comunicación, manifestantes y *whistleblowers*, adoptando una postura especialmente hostil hacia los últimos. (551) [986]

El discurso estigmatizante hacia diversos medios de comunicación y comunicadores es una afectación a la democracia pues genera el imaginario de que el periodista y el periódico son los enemigos que deben ser atacados, por ello este discurso de odio debe ser cuestionado severamente, ya que es un mecanismo de control social que dificulta el quehacer periodístico y la difusión de información veraz y contrastada.

[985] *Ibíd.*
[986] *Ibíd.*

En cuanto a la decisión de Comisión Federal de Comunicaciones de revocar las reglas de 2015 sobre de neutralidad de la red. Las empresas de telecomunicaciones y cable ahora pueden retomar prácticas que impiden el acceso libre a internet, como el bloqueo, la ralentización y la priorización de contenidos. Este tipo de acciones podrían en peligro el acceso libre y sin discriminación a todos los contenidos en internet.

Asimismo, el 16 de noviembre, la Comisión Federal de Comunicaciones autorizó a que emisoras utilicen la nueva tecnología de televisión digital ATSC 3.0. Dicha tecnología permitiría una geolocalización más precisa de las señales de televisión, mejor definición de imagen, programaciones interactivas y mejor precisión en la publicidad. Esta decisión es cuestionada debido a que no prevé la asignación de subsidios para que los usuarios realicen la transición de sus receptores hacia el nuevo estándar y tampoco la realización de un periodo de prueba que permita analizar los riesgos para la privacidad, el uso de la encriptación y el hacking.(632) [987]

La Relatoría Especial reitera que los programas de vigilancia deben concebirse y aplicarse de conformidad con las normas internacionales de derechos humanos. En particular, los Estados deben garantizar que la interceptación, la recopilación y el uso de la información personal estén claramente autorizados por la ley a fin de proteger a las personas de la interferencia arbitraria o abusiva de su privacidad.

En cuanto a México, durante el 2017 se presentaron denuncias de violaciones a la privacidad. En enero, el Diario denunció que un centro de operaciones de la Fiscalía de Chihuahua habría espiado las comunicaciones de políticos, policías, funcionarios, ex servidores públicos, periodistas y empresarios locales. Este espionaje habría sido realizado por medio de equipo israelí. Asimismo, se asegura que a través de un malware llamado Pegasus se pretendía tener acceso a información y a cámaras y micrófonos de celulares para acceder a conversaciones sin conocimiento de los propietarios de los aparatos electrónicos.[988]

Esta Relatoría Especial ha destacado que el ejercicio de la libertad de expresión en internet está estrechamente ligado a la garantía de la privacidad de las personas en la red. La vulneración de la privacidad en las comunicaciones causa un efecto inhibitorio, disminuyendo el pleno ejercicio de la libertad de expresión. Además ha recabado que cualquier mecanismo de interceptación debe estar amparado legalmente y autorizado judicialmente.

La Relatoría Especial para la Libertad de Expresión ha subrayado que en virtud la relación estrecha entre libertad de expresión y privacidad, los Estados deben evitar la implementación de cualquier medida que restrinja, de manera arbitraria o abusiva, la privacidad de los individuos entendida en sentido amplio como todo espacio de intimidad y anonimato, libre de amedrentamiento y de represalias, y necesario para que un individuo pueda formarse libremente una opinión y expresar sus ideas así como buscar y recibir información.

Finalmente, la Declaración Conjunta Sobre Libertad de Expresión y "Noticias Falsas" ("Fake News"), Desinformación Y Propaganda 7 de marzo de 2017, señala que los Estados deben abstenerse de iniciar procesos penales, y de usar leyes sobre difamación

[987] *Ibíd.*
[988] *Ibíd.*

criminal que protegen el honor y la reputación cuando se difunde información sobre asuntos de interés público, sobre funcionarios públicos o sobre candidatos a ejercer cargos públicos. Aunque esta pueda dañar la reputación y afectar la privacidad de personas, o instigar la violencia, la discriminación o la hostilidad hacia grupos identificables de la sociedad. La protección de la privacidad o el honor y la reputación de funcionarios públicos o de personas que voluntariamente se han interesado en asuntos de interés público, debe ser ulterior y estar garantizada únicamente solo a través del derecho civil.

La privacidad se vuelve fundamental para la libertad de expresión, por ello se la ha determinado en su sentido más amplio, esto es:

> "todo espacio de intimidad y anonimato, libre de amedrentamiento y de represalias, y necesario para que un individuo pueda formarse libremente una opinión y expresar sus ideas así como buscar y recibir información. En tal sentido, ha destacado que la protección del derecho a la vida privada implica al menos dos políticas concretas vinculadas al ejercicio del derecho a la libertad de pensamiento y expresión: la protección del discurso anónimo y la protección de los datos personales". (1006)[989]

De lo anteriormente señalado, se concluye que la Libertad de Expresión tiene estrecha relación con la privacidad, pues se nutre y garantiza a través de esta. De tal suerte que, resulta su causa y efecto, puesto que solo quien, a través del anonimato en Internet y de la privacidad, puede acceder al conocimiento de forma libre, y opinar sin temor a las repercusiones puede ejercer su derecho a un discurso anónimo y a su libre expresión.

Si el análisis se limita a la simple difusión no autorizada de información personal, familiar y social de un individuo, la privacidad seguirá siendo el derecho con el cual se protege a la persona de las distintas transgresiones de la era digital y la protección de los datos personales solo será una de las políticas, estrategias o acciones que coadyuva a este objetivo.

Sin embargo, es cada vez más evidente que, esta visión acotada, resulta insuficiente. Pues el devenir de la tecnología ha demostrado que cada día aparecen nuevas e imprevisibles formas de violaciones a los derechos de las personas en línea. Por este motivo, se debe resguardar al individuo en sí mismo, dotarle de protección no solo desde la perspectiva de su intimidad sino del libre desarrollo de su personalidad, de su libertad de decidir, su autodeterminación informativa, este último, elemento esencial del derecho a la protección de datos personales que lo diferencia de la privacidad. Y es que, el derecho a la protección de datos personales se acciona por voluntad de su titular que puede decidir qué tipo de datos, con qué finalidad, por cuánto tiempo, etc. autoriza o no, su procesamiento a un responsable; mientras que, el derecho a la intimidad solo procede cuando un tercero ha realizado una intromisión o difundido información íntima que ha causado perjuicio al titular.

2.1.21 Informe 2018

[989] *Ibíd.*

Conforme la Relatoría Especial 2018 para la libertad de expresión de la CIDH y el relator especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión, se detalla el estado de varios países de América, entre ellos Ecuador.

En el caso argentino, durante el 2018, el gobierno llevó a cabo un proceso de consulta sobre las disposiciones de un anteproyecto de ley de protección de datos. El documento establece disposiciones que se aplicarían expresamente al periodismo (artículo 32): "los datos personales que se procesan solo con fines de periodismo o con fines artísticos o literarios están exentos de cualquier disposición". (101) [990]

En cuanto a Brasil, en junio de 2018, el Tribunal Superior Electoral (TSE) de Brasil tomó su primera decisión con relación a la temática de "*fake news*", que involucraba a la candidata a la Presidencia, Marina Silva: En 48 horas, Facebook debía quitar el contenido considerado falso; y, en 10 días, debía informar sobre el origen de la página responsable por las publicaciones. En agosto, el expresidente Michel Temer sancionó parcialmente la Ley sobre la protección de datos personales. El veto estaban relacionado al inciso II del artículo 23: "los datos del solicitante de acceso a la información" [991] estaban "protegidos y preservados, en los términos de la Ley de Acceso a la Información"[992], lo que prohibía "su divulgación en el ámbito del Poder Público y con las personas jurídicas de derecho privado". (208)[993] Con lo cual se pretendía impedir posibles repercusiones contra el solicitante de información pública.

Respecto a Canadá, la Relatoría determina avances en materia de acceso a la información cuando estipuló que "las reglas sobre las órdenes de búsqueda de información en los medios y órdenes de reproducción debían ser modificadas".(225)[994] Esto en referencia a al caso del periódico Toronto Star contra AG Ontario, en el que, el 27 de abril de 2018, el Tribunal Superior de Justicia de Ontario declaró inconstitucionales las disposiciones de la Ley de Libertad de Información y Protección de la Privacidad que facultaba a los funcionarios a negar el acceso a los documentos del tribunal administrativo que contienen información personal.[995] (239) De esta manera se permite el acceso a esta información por considerarla de interés público. Asimismo, y respecto de procedimientos de desindexación o cancelación de contenidos de funcionarios públicos, la Relatoría Especial señala que:

> […] no pueden utilizarse como un mecanismo preventivo o cautelar para proteger el honor o la reputación. Las personas cuentan con otros procedimientos ante la eventual reparación a los daños ocasionados por la presunta difusión de información considerada falsa, agraviante o inexacta en medios digitales, como el derecho a la rectificación y respuesta y las acciones civiles por daños y perjuicios. Este tipo de acciones resultan menos lesivas del derecho a la libertad de expresión y exigen al demandante a soportar la carga de la prueba de la falsedad o inexactitud de la información divulgada. (250) [996]

[990] *Ibíd.*
[991] *Ibíd.*
[992] *Ibíd.*
[993] *Ibíd.*
[994] *Ibíd.*
[995] *Ibíd.*
[996] *Ibíd.*

De esta manera, este texto coincide con lo señalado por la Relatoría Especial de 2016 respecto de derecho al olvido. La desindexación o cancelación de ser posible no debe incluirse en las legislaciones, de tomarla en cuenta debe estar estrictamente regulada para que no se produzca, a través de él, formas de impunidad a favor de personas públicas que han incurrido en actos de corrupción, por ejemplo.

Relativo a Chile, la Relatoría de Naciones Unidas indica que el Consejo para la Transparencia habría modificado su jurisprudencia al otorgar información sobre cuestiones relacionadas con hechos de acoso en el ámbito laboral y sexual, determinando resguardar la información cuya entrega afecte el cumplimiento de las funciones de la institución requerida y el derecho a la privacidad de personas que intervinieron en los procedimientos administrativos. (281)

Sobre Cuba, en los últimos años el uso de Internet y el desarrollo de medios digitales han permitido, en Cuba, la apertura de espacios para la circulación de información e ideas al margen del control oficial. Se ha constatado la "imposibilidad de acceso a páginas web, plataformas o redes sociales como *Facebook, Twitter, Youtube, Yahoo, MSN o Hotmail*"[997]. (403) Asimismo, la CIDH y su Relatoría Especial informan sobre presuntas actividades de vigilancia a quienes navegan por Internet, usan correo electrónico, mensajería u otras plataformas. (408) La Relatoría Especial reitera al gobierno cubano que "amplíe la conectividad al internet sin restricciones, promoviendo de esta manera el acceso universal a Internet para garantizar el disfrute efectivo del derecho a la libertad de expresión". (409) [998] De esta manera, la libertad de expresión no se garantiza únicamente a través del respeto a la privacidad, la no injerencia a las comunicaciones telefónicas, sino al uso de la red a través de cualquiera de sus aplicaciones, pero además de la accesibilidad a Internet, que debe estar garantizada por los Estados.

En cuanto a Ecuador, durante el mandato del expresidente Rafael Correa se convocó a seguidores a investigar y exponer la identidad de quienes se mostraron abiertamente opositores al régimen. "Tras el descenso de confrontación entre el actual gobierno y medios de comunicación, los periodistas y comunicadores pudieron ejercer su trabajo de manera más segura", señala la Relatoría. A ello se sumó la eliminación del programa 'Enlace Ciudadano' y cambios en la línea editorial de los medios en manos del Estado. (435)[999] Asimismo, varios actores reconocieron que la Ley Orgánica de Comunicación se utilizó como instrumento de persecución y restricción del derecho a la libertad de expresión. (438)[1000] Por ello, se presentaron proyectos de reforma que tienen por objetivo la revisión a las "restricciones para la circulación de distinto tipo de informaciones derivadas de procesos penales o sobre datos personales, ya que no cumplen con el requisito de necesidad en el contexto de una sociedad democrática". (449) [1001] Además, la Relatoría Especial recomienda la eliminación de figuras penales como el linchamiento mediático y la difamación. Privilegiando el cumplimiento del "estándar de la real malicia y la estricta proporcionalidad y razonabilidad de las

[997] *Ibíd.*
[998] *Ibíd.*
[999] Comisión Interamericana de Derechos Humanos (CIDH), "La Relatoría Especial para la libertad de expresión de la CIDH presenta observaciones preliminares tras visita Ecuador", 2018, accedido el 30 de octubre de 2019, https://bit.ly/2AIyOP3
[1000] *Ibíd.*
[1001] *Ibíd.*

sanciones ulteriores de naturaleza civil". (463) [1002] De lo visto, el Ecuador ha presentado mejoras al respeto a la libertad de expresión. La Relatoría Especial ha realizado recomendaciones con las cuales seguir apuntalando las libertades individuales de todos los ciudadanos y el ejercicio de un periodismo libre y responsable.

Respecto a EE.UU, el 11 de abril, el fundador y director de Facebook, Mark Zuckerberg, se presentó ante el Congreso Federal para informar sobre una filtración masiva de datos personales. Durante la comparecencia, el fundador de la red social manifestó que una regulación de la red social sería "inevitable".[1003] En 2017, la Comisión Federal de Comunicaciones (FCC) adoptó revocar las reglas de neutralidad de la red. La Relatoría sostiene que la neutralidad de la red es una condición necesaria para ejercer la libertad de expresión (…). Lo que persigue tal principio es que la libertad de acceso y elección de los usuarios de utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal por medio de Internet no esté condicionada, direccionada o restringida, por medio de bloqueo, filtración, o interferencia". (474) [1004]

Relativo a Guatemala, la CIDH y su Relatoría Especial han indicado que corresponde al Estado garantizar el derecho de todas las personas a acceder a la información pública sobre programas de vigilancia o espionaje, su alcance y los controles existentes. Los organismos señalaron en diversas oportunidades que el uso de cualquier programa o sistema de vigilancia en las comunicaciones privadas debe estar establecido de manera clara y precisa en la ley. (627)

Sobre Jamaica, las organizaciones de la sociedad civil expresaron una serie de preocupaciones sobre un proyecto de ley presentado en 2017, pendiente de tratamiento en el parlamento con respecto a la protección de datos personales. De acuerdo reporte, los medios de prensa serían considerados como "controladores de datos" y estarían obligados a enviar a la eventual oficina del comisionado de información la descripción de los datos personales recibidos, almacenados o procesados. (694)[1005]

Respecto de México, el 27 de junio, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) informó que la Procuraduría General de la República (PGR) está obligada a dar información sobre "el número de averiguaciones previas y casos atraídos por la entonces Fiscalía Especializada para Delitos Cometidos contra Periodistas, de febrero a junio de 2010". [1006] Sobre el caso, los Relatores Especiales recomendaron, en el Informe Especial que el Estado debe llevar un proceso de investigación "independiente sobre la adquisición y el uso de malware (incluido `Pegasus`)". (757)[1007]

Sobre Perú, el 28 de agosto el Ministerio de Justicia y Derechos Humanos de ese país presentó un proyecto de ley que crea el "Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales", que es un organismo público

[1002] *Ibíd.*
[1003] OEA, "Informes Anuales, OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo", 2009, accedido 20 de noviembre de 2017, http://www.oas.org/es/cidh/expresion/informes/anuales.asp.
[1004] *Ibíd.*
[1005] *Ibíd.*
[1006] *Ibíd.*
[1007] *Ibíd.*

técnico especializado con personería jurídica de derecho público interno, que goza de autonomía, técnica, funcional, económica, administrativa y financiera" y que "se encuentra adscrita al Ministerio de Justicia y Derechos Humanos". (886) [1008]

En cuanto a San Cristóbal y Nieves, el 4 de mayo el gobierno habría promulgado una Ley de Protección de Datos Personales que, de acuerdo con el proyecto de 2015, contendría exenciones aplicables a periodistas que recolectan datos personales "procesados únicamente con fines periodísticos, literarios o artísticos", "con miras a la publicación por una persona del material periodístico", cuando el "usuario de los datos cree razonablemente que, teniendo en cuenta la importancia especial del interés público en la libertad de expresión, la publicación sería de interés público"; y cuando "el usuario de los datos cree razonablemente que en todas las circunstancias, el cumplimiento de la disposición respecto de la cual se reclama la exención es incompatible con los fines periodísticos, literarios o artísticos". (949) [1009]

Respecto de Uruguay, a partir de una acción de protección iniciada por el Instituto Nacional de la Niño y el Adolescente del Uruguay (INAU) en la que alegó la violación de los derechos protegidos por el Art. 31 de la LSCA1304, el 26 de febrero el Juzgado Letrado de Primera Instancia en lo Civil de 19º Turno, advirtió a la empresa de comunicaciones Monte Carlo TV S.A. por vulnerar los derechos a la privacidad y a la imagen de dos niñas víctimas de abuso sexual cuyos testimonios se difundieron en el programa "Santo y Seña". (1006) [1010]

Como se ha señalado en múltiples ocasiones, la protección de la privacidad o el honor y la reputación de funcionarios públicos o de personas que voluntariamente se han interesado en asuntos de interés público, debe estar garantizada solo a través del derecho civil. Asimismo, se impida el uso de disposiciones amplias y ambiguas basadas en la "moral" o las "buenas costumbres" que censuren contenidos.

Los efectos de los macrodatos y el aprendizaje automático, en particular cuando se aplican a fines predictivos y preventivos, sobre el goce del derecho a la privacidad y otros derechos humanos; y la regulación de los mercados de tecnología de vigilancia. Esta relatoría hace hincapié en señala que las situaciones de conflicto no deben ser utilizadas para justificar el aumento de la vigilancia estatal. (301) Un entorno abierto, seguro, estable, accesible y pacífico en el ciberespacio es sumamente importante para la realización del derecho a la privacidad en la era digital.

En la Declaración Conjunta sobre la Independencia y la Diversidad de los Medios de Comunicación en la Era Digital, se recomienda a los Estados a crear entornos propicios para:

> […] buscar, recibir e impartir información e ideas (libertad de expresión), incluso con las siguientes medidas: i. asegurar que haya leyes sobre el derecho de acceso a la información pública y que se exija su cumplimiento; ii. promover el acceso universal a

[1008] *Ibíd.*
[1009] *Ibíd.*
[1010] *Ibíd.*

> la Internet; iii. proteger de manera adecuada la privacidad y los datos personales, incluso posibilitando el uso anónimo de tecnologías digitales […][1011]

Esta declaración reconoce la complejidad del resguardo de los derechos humanos en internet ante el avance de tecnologías como localización, de formas intrusivas de vigilancia por el Estado, de la desindexación de contenido por razones de privacidad, la desinformación y la brecha informática en los países y entre ellos.

Sobre amenazas tecnológicas, la declaración recomienda que:

> a. La vigilancia digital solo debe ser posible por disposición legal, necesaria, proporcional para proteger un interés legítimo del Estado.
> b. No se pretenderá identificar fuentes periodísticas confidenciales directa o indirectamente a través del uso de medios digitales, con el objetivo de llevar a cabo investigaciones penales.
> c. El derecho al olvido no debiera ser parte de la legislación, pero si el país lo incluye esta deberá ser estricta, dispuesta a través de términos claros y específicos, valorado a través del debido proceso por un juez.
> d. Los Estados deberá proteger los sistemas de comunicaciones digitales contra ataques cibernéticos y de reforzar la seguridad digital, en especial respecto de individuos que ejercen su derecho a la libertad de expresión. [1012]

De este informe se colige que, sobre derechos humanos en la era digital otras latitudes han desarrollado derechos y principios con los que intentan proteger la dignidad del individuo. Lamentablemente en este lado del hemisferio, estos derechos son un reto para la garantía de derechos, puesto que figuras como la protección de datos, aún no se visualiza como autónoma e independiente, sino que son solo una estrategia o acción para proteger la privacidad. Asimismo, el anonimato, la neutralidad de la red, el acceso a internet no se consideran aún como derechos digitales sino como recomendaciones insoslayables para garantizar la privacidad y por ende la libertad de expresión.

Sin duda, nos encontramos ante el inminente nacimiento de nuevos derechos, que paulatinamente irán definiendo su propio contenido esencial, su propio fundamento. Que dejarán de ser vistos como meros habilitantes de otros derechos y pasarán a ser condiciones ineludibles para que la persona virtual pueda desarrollarse de forma libre en entornos virtuales.

2.1.22 Principales conclusiones de los informes de la Relatoría para la libertad de expresión, respecto de intimidad, privacidad y *habeas data*

Acerca de los 21 informes anuales de la Relatoría para la Libertad de Expresión, se colige que, si bien su contenido se direcciona al ejercicio de la libertad de expresión; sin embargo, debido al desarrollo de las TIC, se hace mención a la intimidad y a la privacidad como derechos base y se enumera varias nuevas formas de transgresión, así también, varios mecanismos, estrategias y políticas que se sugieren implementar a los Estados partes para proteger a las personas.

[1011] *Ibíd.*
[1012] *Ibíd.*

En el informe del año 2001 si bien se menciona al *habeas data* como garantía que permite a las personas acceder, actualizar o rectificar información sobre sí mismas o sus bienes, que se encuentran contenidas en bases de datos o registros públicos. Esta relatoría otorga otra función al *habeas data*. Esto es, como mecanismo de control de posibles abusos por parte del Estado respecto de injerencias arbitrarias a la privacidad de las personas.

Para el año 2005 y en adelante, la principal recomendación radica en que al utilizar la garantía del *habeas data* no se deberá limitar o restringir la búsqueda, difusión o investigación de información de interés público. Asimismo, el informe de 2008 se reconoce al *habeas data* como el mecanismo fundamental para evitar la difusión y divulgación de datos sensibles o errores que puedan afectar la reputación, intimidad u otros derechos humanos. En el informe 2010 se desarrolla el contenido y alcance del *habeas data.* En el informe de 2012 se hace alusión a que los datos privados, íntimos o reservados de una persona, que no sean de relevancia pública, no pueden ser ni capturados y archivados ni divulgados, pues se encuentran protegidos por el derecho a la intimidad.

Por eso, se puede concluir que, hasta el 2012, en los citados informes:

1. No se distingue entre privacidad e intimidad, pues estos se centran en analizar las ofensas al honor o la citada intimidad que se derivan de la investigación o difusión de información de interés público y la recomendación de derogar las legislaciones, los delitos de desacato, calumnias e injurias.
2. No hay evolución en la diferenciación entre privacidad e intimidad.
3. Sobre *habeas data* se determina que, a través de él, las personas pueden acceder a información sobre sí mismas o sobre sus bienes contenida en bases de datos o registros públicos y privados, y en caso de ser necesario actualizar, rectificar o suprimir dicha información.
4. Respecto del derecho a la protección de datos personales, este no ha sido reconocido como autónomo por lo que tampoco se ha desarrollado.

Ahora bien, es en los siguientes informes, los dictados desde el año 2013 hasta el 2018, que se empieza a identificar la problemática del uso inadecuado de los datos y cómo esta actuación menoscaba la libertad de expresión, de pensamiento y por ende la democracia misma.

Así pues, el informe 2013, es el primero que aborda la correlación inherente y directa entre libertad de expresión, ciberseguridad, protección de datos personales, imagen y especialmente, privacidad; así como, confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos. Asimismo, determina que la recolección de metadatos telefónicos invade expectativas razonables de privacidad. Y es que, el 18 de diciembre de este año, la Asamblea General de la ONU, dicta la resolución "El derecho a la privacidad en la era digital". Para la Relatoría Especial, cuyos informes sirvieron de fundamento para la resolución, es necesario respetar y proteger la libertad de expresión en el contexto de las comunicaciones digitales, a través del equilibrio entre seguridad nacional y privacidad; así como instar a los estados a desarrollar regímenes legales y técnicos de protección de datos personales para permitir un almacenamiento, tratamiento y difusión adecuada.

El informe 2014 se determina que cuando se realiza injerencias a la privacidad para la investigación delitos y temas de seguridad nacional, la normativa debe establecer que ésta, solo es posible, previa autorización de la ley y mediante orden dictada por juez competente, además de respetar otras garantías vinculadas al debido proceso.

En cuanto al informe 2015, se dimensiona la importancia de la protección de las personas respecto de la acumulación masiva de datos personales que pudiere ser lesiva para la privacidad y por ende para la libertad de expresión. Es evidente que los datos personales son sustanciales para el desarrollo de la sociedad y que pueden ser usados positiva o negativamente. Por ello, el Consejo de Derechos Humanos creó el mandato del Relator Especial sobre el derecho a la privacidad en julio de 2015[1013] con la finalidad de monitorear los riesgos y problemáticas que pudieran llegar afectar los derechos humanos de los individuos en su interrelación con internet.

Respecto del informe 2016, se determina al Estado, en su rol de garante, como a los particulares, en su rol de usuarios, como posibles transgresores o víctimas de derechos humanos, en especial de la privacidad, en la era digital. En este sentido, así como aparecen nuevos problemas jurídicos, emergen nuevos derechos para solucionar estas realidades como: la ciberseguridad, el anonimato, el cifrado o la protección de datos personales. Esta última, no se reconoce aun como derecho pero es evidente que sus elementos esenciales se encuentran en debate, pues se vuelve indispensable regular la captura, análisis, uso general de la información personal y traspaso, no solo desde la perspectiva de propiedad del dato, sino desde el reconocimiento del titular y sus derechos de autodeterminación informativa.

En cuanto al informe 2017, se insiste en la estrecha relación entre libertad de expresión y privacidad como garantía de un estado democrático. Ya que, solo a través del anonimato y de la privacidad, se puede acceder de forma libre a internet y a la información, se puede opinar sin temor a las repercusiones y ejercer libertad de expresión.

Finalmente, en el informe 2018 se evidencia el aumento de la interceptación y de la vigilancia indirecta o masiva; la recolección y retención masiva de datos personales, incluidos los metadatos telefónicos, con finalidades como el orden y la seguridad pública; y, la incorporación del derecho al olvido; todo lo cual afecta la privacidad de los individuos e incide directa en la libertad de expresión.

La privacidad resulta sustancial pues solo si el ciudadano se siente libre de amedrentamientos y de represalias, es decir cuando no se percibe vigilado, por parte del Estado o de particulares, puede ejercer plenamente su derecho a ser informado, a su libre expresión en todas sus manifestaciones: opinión, libre pensamiento, convocar a movilizaciones sociales, entre otras.

De lo analizado en los distintos informes se colige que para la Relatoría Especial y la Asamblea General de las OEA, la privacidad es el derecho con el cual se protege a la

[1013] Asamblea General de las Naciones Unidas, Resolución 28/16 sobre el derecho a la privacidad en la era digital, 1 de abril de 2015, accedido el 14 de septiembre de 2019, Resolución https://www.google.com/search?q=resoluci%C3%B3n+del+Consejo+de+Derechos+Humanos+28%2F16&oq=resoluci%C3%B3n+del+Consejo+de+Derechos+Humanos+28%2F16&aqs=chrome..69i57j33l2.982j0j7&sourceid=chrome&ie=UTF-8

persona en la era digital. La privacidad entendida como un derecho de los individuos a una esfera de desarrollo autónomo, de interacción y libertad, así como a estar exentos de la intervención del Estado y de otros individuos no invitados. Este derecho es amplio, no solo abarca la información sustantiva contenida en las comunicaciones, sino también en metadatos. El simple hecho que se generen y reúnan datos relativos a la identidad, la familia o la vida de una persona ya afecta a su derecho a la privacidad. Es decir, el derecho a la privacidad es fundamental para el goce y el ejercicio de los derechos humanos dentro y fuera de Internet. Pero debido al almacenamiento, procesamiento y automatización masiva e inmediata, la privacidad de la información tiene especial importancia en el entorno digital.

Ahora bien, la reglamentación excesiva de la privacidad también puede poner limitaciones indebidas a derechos como la libertad de expresión. En tal sentido, tal como se ha mencionado en informes anteriores, no puede ser invocada para evitar el acceso a información de interés público.

La visión acotada de la privacidad como derecho sustancial para la defensa de las transgresiones en la era digital, debe ser paulatinamente superada puesto que para que la protección de la dignidad humana en entornos digitales sea completa se requiere del reconocimiento de otros derechos digitales, en especial la protección de datos personales. Y es que, en la medida en que los cambios tecnológicos se produzcan y se expliciten nuevas formas de transgresiones a los derechos humanos, la privacidad, desde la perspectiva del deber de no realizar injerencias arbitrarias al espacio íntimo de las personas resulta no ser suficiente. Así como tampoco lo es, la simple regulación sobre las formas adecuadas de tratamiento de los datos personales, pues el centro no solo es el dato personal como activo económico sino como centro de un sistema integral de protección y garantía de otros derechos fundamentales, incluidos los nuevos derechos digitales.

2.2 Corte Interamericana de Derechos Humanos (Corte IDH)

La Corte Interamericana de Derechos Humanos no ha dictado resoluciones sobre protección de datos personales; sin embargo, ha dictado varias respecto de libertad de expresión, vida privada, intimidad y honra. En este sentido, a continuación se extractan varias resoluciones que pueden servir de orientación para comprender el enfoque de este Alto Tribunal en la comprensión de estos temas.

2.2.1 Olmedo Bustos y otros vs. Chile; sentencia de 5 de febrero del 2001

Este caso habla sobre la protección del honor como medida precautelar. Se considera que el derecho al honor y la libertad de expresión se encuentran en conflicto, debido a que al darle un carácter cautelar se tiende a considerar que podría ser una medida de censura previa. En su análisis, la Corte IDH manifiesta que existen dos tipos de derechos humanos: aquellos que corresponden a la dignidad como al derecho a la vida, al honor, a la intimidad, entre otros, y los derechos humanos de medio como la libertad de opinión, información y expresión.[1014]

[1014] OEA, "OEA - Organización de los Estados Americanos".

Se establecen que existen tres mecanismos alternativos mediante los cuales se pueden imponer restricciones al ejercicio de la libertad de expresión: las responsabilidades ulteriores, la regulación del acceso de los menores a espectáculos públicos y a la obligación de impedir la apología del odio religioso.

En ese caso, se prohibió la proyección de la película "La última tentación de Cristo", ya que se buscaba defender la defensa del derecho al honor y reputación de Jesucristo; al respecto se ha manifestado que el honor de los individuos debe ser protegido sin perjudicar el ejercicio de la libertad de expresión y del derecho a recibir información.[1015]

2.2.2 Ivcher Bronstein vs. Perú; sentencia de 2 febrero del 2001

Este caso se trata de un ciudadano peruano por naturalización quien era accionista de un canal de televisión, en el cual se transmitían programas que realizaban críticas al Gobierno peruano, lo que trajo como consecuencia que se le revocara la ciudadanía y, por ende, perdiera el control de su canal.

No se menciona la protección de datos, el *habeas data*, la privacidad, la honra o la intimidad.[1016]

2.2.3 Herrera Ulloa vs. Costa Rica; sentencia de 2 julio del 2004

Un periodista que había publicado varios artículos reproduciendo información acerca de actuaciones ilícitas de un diplomático de Costa Rica fue condenado a cuatro cargos con difamación.

La Corte IDH analizó que el honor al igual que la libertad de expresión son derechos fundamentales de las personas, que debe de existir un balance entre ellos y que no se puede limitar o restringir la investigación o difusión de interés social.

Se estableció como criterio que las sanciones penales en los casos en el que se afecta el honor son desproporcionadas y vulneran el derecho a la libertad de expresión, por lo que se requirió que se anulen dichos procesos criminales en contra del periodista.[1017]

2.2.4 Ricardo Canese vs. Paraguay; sentencia de 31 de agosto del 2004

En 1993, durante la campaña presidencial, el candidato Ricardo Canese hizo varias declaraciones en medios de comunicación en contra del candidato Juan Carlos Wasmosy. Este candidato fue procesado y sentenciado a cuatro meses de prisión.

La Corte IDH manifestó que esta condena era desproporcionada y que vulneraba el derecho a la libertad de expresión ya que, si bien es necesario proteger el derecho al

[1015] Ibíd.
[1016] Ibíd.
[1017] Ibíd.

honor, las sanciones penales son exageradas y limitan el pleno ejercicio del derecho a la libertad de expresión.[1018]

2.2.5 Palamara Iribarne vs. Chile; sentencia de 22 de noviembre del 2005

El accionante era un exmilitar chileno quien había escrito un libro que criticaba fuertemente a la armada nacional. Este libro originó un proceso militar penal. La Corte IDH ordenó que se reformara la ley en Chile respecto a la libertad de expresión y la reparación a la víctima.

Dentro de este caso no se hace mención a la honra privacidad, protección de datos personales o la acción de *habeas data*.[1019]

2.2.6 Kimel vs. Argentina; sentencia de 2 mayo del 2008

Eduardo Kimel criticó a un juez respecto de sus actuaciones dentro de una investigación sobre masacre, lo que originó un proceso penal. Finalmente, la Corte IDH manifestó que el proceso era desproporcionado, ya que las sanciones penales no son la vía óptima para proteger el honor de las personas. Concluyó que el derecho al honor debe estar en balance con el derecho a la libertad de expresión.[1020]

2.2.7 Tristán Donoso vs. Panamá; sentencia de 27 de enero del 2009

Un abogado aseguró en una conferencia de prensa que un agente del Estado había interceptado ilegalmente conversaciones privadas y las había divulgado.

Dentro de este caso, la Corte IDH analizó la violación del derecho a la vida privada de la presunta víctima, por la interceptación y grabación de una conversación telefónica, difusión de su contenido, y no identificar y sancionar a los responsables. Además, se analizó el derecho al honor y a la desproporcionalidad de las sanciones penales, que se refieren a la protección del derecho de honor, estableciéndose que las sanciones civiles son el mecanismo efectivo para garantizarlo.[1021]

Dicha resolución considera que el artículo 11 de la Convención también incluye la protección de las comunicaciones profesionales pues la privacidad incluye el desarrollo de relaciones entre personas y precisamente la vida profesional de un individuo. Dicha resolución señala que el derecho a la vida privada no es absoluto. Puede ser restringido por los Estados siempre, basado en una ley que habilite, una autoridad judicial dicte una orden que persiga un fin legítimo y se cumpla con los requisitos de idoneidad, necesidad y proporcionalidad.

[1018] Ibíd.
[1019] Ibíd.
[1020] Ibíd.
[1021] Ibíd.

2.2.8 Ríos y otros vs. Venezuela; sentencia de 28 de enero del 2009

En Venezuela se realizaron distintos actos públicos y privados que restringieron la labor periodística de los trabajadores del canal RCTV. Al respecto, la Corte IDH manifestó que no encontró las responsabilidades del Estado respecto a estos hechos, y ordenó que se conduzcan eficazmente las investigaciones y procesos penales por hechos de violencia contra periodistas, así como la adopción de medidas necesarias para evitar restricciones indebidas.[1022]

2.2.9 Perozo y otros vs. Venezuela; sentencia de 28 enero 2009

Algunos funcionarios públicos dieron declaraciones que obstaculizaron el ejercicio de la libertad de expresión en contra de personas vinculadas al canal de televisión Globo Visión. Nada se menciona sobre el *habeas data*, la honra, intimidad o protección de datos personales, ya que se analizaron las medidas estatales de prevención e investigación de actos violentos en contra de periodistas.[1023]

2.2.10 Usón Ramírez vs. Venezuela; sentencia de 20 noviembre del 2009

Usón emitió opiniones críticas en un programa televiso respecto del caso de un grupo de soldados que resultaron heridos en una instalación militar, por lo que fue condenado por el delito de injuria sobre la Fuerza Armada Nacional.

La Corte IDH manifestó en su análisis que la protección a la honra no puede darse por la vía penal, ya que se vulnera la proporcionalidad con relación a la libertad de expresión.[1024]

2.2.11 Manuel Cepeda Vargas vs. Colombia; sentencia de 26 de mayo 2010

El senador Manuel Cepeda Vargas, líder de la dirección Nacional del Partido Comunista Colombiano, fue asesinado. La Corte IDH analizó el derecho a la vida y a la libertad de expresión.

Dentro de este caso no se hace mención a la honra privacidad, protección de datos personales o la acción de *habeas data*.[1025].

2.2.12 Gómez Lund y otros vs. Brasil; sentencia de 24 de noviembre del 2010

Este cargo versa sobre la detención arbitraria, tortura y desaparición forzada de 70 personas como resultado de operaciones del ejército brasileño, con el objetivo de erradicar la guerrilla de Araguaia. La Corte IDH analizó el derecho a la libertad, a la vida, en relación con el de libertad de expresión. Puntualmente, desarrolló sobre el derecho de acceso a la información pública.

[1022] Ibíd.
[1023] Ibíd.
[1024] Ibíd.
[1025] Ibíd.

Dentro de este caso, no se hace mención a la honra, privacidad, protección de datos personales o la acción de *habeas data*.[1026]

2.2.13 Fontevecchia D'Amico vs. Argentina; sentencia de 29 de noviembre del 2011

Este caso hace referencia a la condena civil impuesta a los actores por responsabilidad ulterior debido a la publicación de dos artículos en 1995. Por la publicación de una noticia sobre la existencia de un hijo no reconocido de Carlos Menen, presidente de Argentina, y la relación que tenía con su madre una diputada del citado país. La Corte analizó que los funcionarios públicos están más expuestos al escrutinio y crítica del público, y que sus actividades salen del dominio de la esfera privada para insertarse en la esfera del debate público. La protección a la privacidad no puede limitar o restringir la investigación o difusión de información de interés social, por lo que no cabe ninguna sanción a los editores.[1027]

En este sentido, la citada jurisprudencia reconoce que la privacidad protege al menos cuatro bienes jurídicos directamente relacionados con la libertad de expresión: intimidad; autodeterminación informativa; secreto y prohibición de divulgación de datos personales sin autorización del titular; y, la propia imagen.

2.2.14 González Medina y Familiares vs. República Dominicana; sentencia de 27 de febrero del 2012

El periodista Narciso Gonzales Medina había publicado un artículo de opinión en la revista denominada *La Muralla*, en donde denunciaba la corrupción y fraude electoral, dando como resultado que días después se produjera su desaparición forzada. Esto ocurrió en el año 1994, por lo que dentro de esta sentencia se analizó el derecho a la vida, libertad e integridad personal.

Dentro de este caso no se hace mención a la honra, privacidad, protección de datos personales o la acción de *habeas data*.[1028]

2.2.15 Vélez Restrepo y Familiares vs. Colombia; sentencia de 3 de septiembre del 2012

El periodista Luis Gonzalo Richard Vélez Restrepo firmaba una manifestación en la cual soldados del Ejército Nacional atacaban a los manifestantes; posteriormente recibió varias amenazas, fue sujeto de hostigamiento y presuntamente se intentó privarle de manera arbitraria de la libertad. Dentro del análisis que hace la Corte IDH se desarrolla sobre la falta de seguridad que sufren los periodistas a la hora de ejercer su derecho a la libertad de expresión.

[1026] Ibíd.
[1027] Ibíd.
[1028] Ibíd.

Dentro de este caso no se hace mención a la honra, privacidad, protección de datos personales o la acción de *habeas data*.[1029]

2.2.16 Uzcátegui y Otros vs. Venezuela; sentencia de 3 de septiembre del 2012

Este caso trata sobre la situación de vulnerabilidad que viven los periodistas y defensores de derechos humanos en Venezuela; se habla sobre el derecho a la vida, libertad de expresión y a la integridad personal.

Dentro de este caso no se hace mención a la honra, privacidad, protección de datos personales o la acción de *habeas data*.[1030]

2.2.17 Artavia Murillo y Otros Vs. Costa Rica, sentencia de 28 de noviembre de 2012

Costa Rica prohibió la práctica de la fecundación *in vitro*. La pareja Artavia Murillo, entre otras varias consideraciones señaló que esta "prohibición absoluta constituyó una injerencia arbitraria en los derechos a la vida privada y familiar y a formar una familia". Es decir, una transgresión flagrante al artículo 11 de la Convención Americana. Ya que, la decisión de formar o no una familia se produce en el ámbito privado. (138) Los derechos afectados serían la intimidad, la autonomía de la voluntad en el ámbito familiar y el libre desarrollo de la personalidad. (139)

Respecto de esta afirmación, la Corte Interamericana ha sostenido que:

> […] el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública. Además, esta Corte ha interpretado en forma amplia el artículo 7 de la Convención Americana al señalar que éste incluye un concepto de libertad en un sentido extenso como la capacidad de hacer y no hacer todo lo que esté lícitamente permitido. (…) En otras palabras, constituye el derecho de toda persona de organizar, con arreglo a la ley, su vida individual y social conforme a sus propias opciones y convicciones. La libertad, definida así, es un derecho humano básico, propio de los atributos de la persona, que se proyecta en toda la Convención Americana. Asimismo, la Corte ha resaltado el concepto de libertad y la posibilidad de todo ser humano de auto-determinarse y escoger libremente las opciones y circunstancias que le dan sentido a su existencia, conforme a sus propias opciones y convicciones. (…) El ámbito de protección del derecho a la vida privada ha sido interpretado en términos amplios por los tribunales internacionales de derechos humanos, al señalar que éste va más allá del derecho a la privacidad. La protección a la vida privada abarca una serie de factores relacionados con la dignidad del individuo, incluyendo, por ejemplo, la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales. El concepto de vida privada engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y

[1029] Ibíd.
[1030] Ibíd.

> con el mundo exterior. (…) La vida privada incluye la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás, y es una condición indispensable para el libre desarrollo de la personalidad. (143)

Este sentido amplio de comprensión del derecho a la vida privada ha sido base para sostener que la "decisión de ser o no madre o padre es parte del derecho a la vida privada e incluye, en el presente caso, la decisión de ser madre o padre en el sentido genético o biológico".

Sin duda, esta resolución muestra una interpretación amplia del derecho a la vida privada que debe ser emulado para otros ámbitos, como el digital. De tal suerte que, la autodeterminación informativa que es elemento sustancial del derecho a la protección de datos personales, bajo la misma amplia compresión del derecho, se extrapole a la vida privada.

Pero para que la protección sea integral debe entenderse a la vida privada y por ende a la privacidad, como manifestación positiva, es decir no se necesita de un tercero que transgreda el derecho sino que basta con que el titular desee por sí mismo y bajo sus propios términos ejercer el derecho. Tampoco se requiere la identificación de la naturaleza de la información, esto es que la misma sea de aquella considerada íntima o privada sino que sea suficiente que sea de aquella que identifica o hace identificable a la persona. De tal suerte que, toda información personal que se acumule afecte su privacidad sin alusión a la naturaleza íntima, privada o notoria de dicha información.

2.2.18 Norin Catriman y otros (dirigentes, miembros y actividades del pueblo indígena Mapuche) vs. Chile; sentencia de 29 de mayo de 2014

Este caso se refiere al proceso penal que se les siguió a los accionantes, debido a actos de terrorismo en el contexto de la protesta social por la recuperación de territorios ancestrales.

Dentro de este caso no se hace mención a la honra, privacidad, protección de datos personales o la acción de *habeas data*.[1031]

2.2.19 Granier y Otros (Radio Caracas Televisión) vs. Venezuela; sentencia de 22 de junio del 2015

El 27 de mayo del 2007, el canal de televisión Radio Caracas Televisión cerró en consecuencia de la no renovación de la licencia debido a que no expresaba opiniones afines al Gobierno. Dentro de esta sentencia se analizó el derecho a la libertad de expresión en relación al derecho de no discriminación.

Dentro de este caso no se hace mención a la honra, privacidad, protección de datos personales o la acción de *habeas data*.[1032]

[1031] Ibíd.
[1032] *Ibíd.*

2.2.20 López Lone y otros vs. Honduras; sentencia de 5 octubre de 2015

Dentro de este caso la corte reconoce la relación que existe entre los derechos políticos y la libertad de expresión, siendo este derecho un elemento esencial de la democracia. Dentro de este caso no se hace mención la honra, privacidad, protección de datos personales o la acción de *Habeas Data*[1033].

2.2.21 Sobre la vida privada

De las resoluciones analizadas se puede concluir que la Corte Interamericana de Derechos Humanos desarrolla ampliamente el contenido esencial del derecho a la libertad de pensamiento y expresión incluida las interrelaciones con otros derechos fundamentales como el honor y la imagen.

Ahora bien, sobre privacidad la mayoría de las resoluciones analiza este derecho a la luz de la necesidad de encontrar un equilibrio entre la vida privada y la libertad de expresión, reconociendo que estos "dos derechos fundamentales garantizados en la Convención Americana y de la mayor importancia en una sociedad democrática".[1034] (50)

A continuación sintetizamos la postura e interpretación que sobre vida privada la Corte Interamericana de Derechos Humanos ha realizado en varias de sus resoluciones:

a) *La vida privada no puede sufrir invasiones o agresiones abusivas o arbitrarias:* La Corte considera que el artículo 11 de la Convención tiene su aplicación directa en el ámbito de la vida privada, pues prohíbe toda injerencia arbitraria o abusiva, por parte de un tercero o del Estado,(194) [1035] a los "diversos ámbitos de la misma como la vida privada de sus familias, sus domicilios o sus correspondencias" [1036], así como la posibilidad de tomar decisiones relacionadas con diversas áreas de la propia vida libremente, tener un espacio de tranquilidad personal, mantener reservados ciertos aspectos de la vida privada y controlar la difusión de información personal hacia el público. (48) [1037]
b) *Desarrolla el contenido de la privacidad:* La privacidad protege al menos cuatro bienes jurídicos directamente relacionados con la libertad de expresión: intimidad; autodeterminación informativa; secreto y prohibición de divulgación de datos personales sin autorización del titular; y, la propia imagen.[1038]

   La Corte Interamericana de Derechos Humanos además precisó que, la vida privada es un concepto amplio que no es susceptible de definiciones exhaustivas

[1033] *Ibíd.*
[1034] CORTE INTERAMERICANA DE DERECHOS HUMANOS, "Caso *Fontevecchia y D'amico* vs. Argentina", Sentencia de 29 de noviembre de 2011", accedido el 2 de noviembre de 2019, http://www.corteidh.or.cr/docs/casos/articulos/seriec_238_esp.pdf
[1035] CORTE INTERAMERICANA DE DERECHOS HUMANOS, Caso de las masacres de Ituango vs. Colombia, sentencia de 1 de julio de 2006, accedido el 2 de noviembre de 2019, http://Www.Corteidh.Or.Cr/Docs/Casos/Articulos/Seriec_148_Esp.Pdf
[1036] CORTE INTERAMERICANA DE DERECHOS HUMANOS, "Caso *Fontevecchia Y D'amico* Vs. Argentina"
[1037] CORTE INTERAMERICANA DE DERECHOS HUMANOS, "Caso *Fontevecchia y D'amico* vs. Argentina"
[1038] CORTE INTERAMERICANA DE DERECHOS HUMANOS, "Caso *Fontevecchia y D'amico* vs. Argentina"

y comprende, entre otros ámbitos protegidos, la vida sexual y el derecho a establecer y desarrollar relaciones con otros seres humanos[1039].

La vida privada incluye la forma en que el individuo se ve a sí mismo; cómo y cuándo decide proyectarse a los demás, respecto de aspectos de su identidad física y social.[1040] Por lo que, la distribución de contenido producto de *sexting* entre terceros infiere un daño a la vida privada de la persona, alterando la percepción de esta persona en sociedad.[1041]

c) *Criterios que habilitan la difusión de información privada:* Para el funcionamiento de una sociedad democrática, se relevan dos criterios que habilitan la difusión de información sobre "eventuales aspectos de la vida privada: a) el diferente umbral de protección de los funcionarios públicos, más aún de aquellos que son elegidos popularmente, respecto de las figuras públicas y de los particulares, y b) el interés público de las acciones que aquellos realizan ".[1042] En este sentido, en estos casos, prima el derecho a la libertad de expresión por encima de la privacidad.

d) *No se requiere autorización para el uso de imágenes de funcionarios públicos:* En este sentido, la Corte señala que "no toda publicación de imágenes requiere el consentimiento de la persona retratada. Esto resulta aún más claro cuando las imágenes se refieren a quien desempeña el más alto cargo ejecutivo de un país, dado que no sería razonable exigir que un medio de comunicación deba obtener un consentimiento expreso en cada ocasión que pretenda publicar una imagen del Presidente de la Nación".[1043] En este caso, se considera nuevamente que prima la libertad de expresión por sobre el derecho a la privacidad cuando se refiere a funcionarios públicos.

e) *El Estado tiene la obligación de garantizar el derecho a la vida privada mediante acciones positivas:* Si bien, se aclara que no es suficiente que el Estado asuma una postura de abstención de afectar la privacidad sino que, debe brindar la protección de la ley contra aquellas injerencias. "En consecuencia, el Estado tiene la obligación de garantizar el derecho a la vida privada mediante acciones positivas, lo cual puede implicar, en ciertos casos, la adopción de medidas dirigidas a asegurar dicho derecho protegiéndolo de las interferencias de las

[1039] F. BUENO DE MATA, *Fodertics 3.0: estudios sobre nuevas tecnologías y justicia* (Granada: Editorial Comares, 2015), 193. *Corte IDH. Caso Rosendo Cantú y otra vs. México. Excepción preliminar, fondo, reparaciones y costas, Sentencia de 31 de agosto de 2010, Serie C No. 216, párr. 119. Caso Fernández Ortega y otros vs. México, Excepción preliminar, fondo, reparaciones y costas, Sentencia de 30 de agosto de 2010, Serie C No. 215, párr. 129. Caso Atala Riffo y Niñas vs. Chile, Fondo, reparaciones y costas, Sentencia de 24 de febrero de 2012, Serie C No. 239, párr. 162, citando TEDH. Caso X y Y vs. Países Bajos (No. 8978/80), Sentencia de 26 de marzo de 1985, párr. 22. Caso Niemietz, supra nota 159, párr. 29.*

[1040] CORTE INTERAMERICANA DE DERECHOS HUMANOS, Caso Artavia Murillo y otros ("fecundación in vitro") vs. Costa Rica, sentencia de 28 de noviembre de 2012, accedido el 2 de noviembre de 2019, http://www.corteidh.or.cr/docs/casos/articulos/seriec_257_esp.pdf

[1041] F. BUENO DE MATA, *Fodertics 3.0: estudios sobre nuevas tecnologías y justicia*, 194.

[1042] CORTE INTERAMERICANA DE DERECHOS HUMANOS, Caso *Fontevecchia y D'amico* vs. Argentina.

[1043] Ibíd.

autoridades públicas así como también de las personas o instituciones privadas, incluyendo los medios de comunicación". (49) [1044]

f) *Privacidad y su vínculo con la libertad:* La protección del ámbito de la privacidad está estrictamente vinculada con el derecho a la libertad personal contemplado en el artículo 7 de la Convención Americana, adoptando un concepto amplio de la libertad como "la capacidad de hacer y no hacer todo lo que esté lícitamente permitido" (187).[1045] Ya que, bajo la premisa de que todo lo que no está prohibido está permitido, se pude ejercer libremente decisiones como aquellas relativas a conformar o no una familia o ser padres biológicos o no.

g) *Vida privada y domicilio:* Se vinculan directamente porque es en el domicilio que se puede desarrollar libremente la vida privada. "La Corte Europea de Derechos Humanos, (…) ha tratado el tema de la propiedad privada conjuntamente con el derecho al respeto de la vida privada y familiar y del domicilio, lo cual es garantizado por el artículo 8 del Convenio Europeo de Derechos Humanos." (195) [1046] Y es que solo, quien goza de un espacio físico del cual sea titular, posesionario o tenedor puede disfrutar de los beneficios de la privacidad y cobijo que el domicilio le brinda. Por ello es que la Corte Interamericana, considera que es un "ámbito propio o <<natural>> de desarrollo personal y familiar del individuo"[1047]. En este sentido, se ha concebido el derecho a la inviolabilidad del domicilio, como la falta de consentimiento o de orden judicial que permita o justifique su intromisión.

h) *Vida privada y correspondencia:* Tradicionalmente el artículo 11 de la Convención protege la correspondencia, pues se considera como parte de la vida privada de un individuo. Por ello, el citado artículo, incluye la protección de las comunicaciones profesionales pues la privacidad incluye el desarrollo de relaciones entre personas y precisamente la vida profesional de un individuo. En este sentido, se protege a las personas de la vigilancia o interceptación de comunicaciones, a menos que, el Estado, basado en una ley, en una orden de autoridad judicial competente, apegado a un fin legítimo, cumple con los requisitos de idoneidad, necesidad y proporcionalidad.[1048]

De las resoluciones estudiadas se concluye que es la Corte Interamericana como tribunal de derechos humanos de las Américas la que debe ir marcando el contenido, alcance y aplicabilidad de la privacidad como derecho. Lo que pone en evidencia que el contenido esencial del derecho a la privacidad sigue en desarrollo.

Para la comprensión de este derecho la Corte Interamericana ha vinculado a la privacidad con otros derechos como: libertad de expresión, honor, buen nombre, inviolabilidad del domicilio, inviolabilidad de la correspondencia y libertad. Pues, solo

[1044] *Ibíd.*
[1045] CORTE INTERAMERICANA DE DERECHOS HUMANOS, Caso Artavia Murillo y otros.
[1046] CORTE INTERAMERICANA DE DERECHOS HUMANOS, Caso de las masacres de Ituango vs. Colombia.
[1047] *Ibíd.*
[1048] CORTE INTERAMERICANA DE DERECHOS HUMANOS, Caso Tristán Donoso vs. Panamá, sentencia de 27 de enero de 2009, accedido el 2 de noviembre de 2019, http://www.corteidh.or.cr/docs/casos/articulos/seriec_193_esp.pdf

a través de una visión integral que, a través de la interrelación con otros derechos que limiten y delineen su contenido esencial, se puede garantizar su efectiva vigencia.

Y es que, la privacidad encuentra sus límites en la libertad de expresión y por ende información de interés público puede ser difundida aun cuando pertenezca a la esfera familiar o personal de un individuo. Asimismo, la correspondencia y el domicilio son actividades y espacios en los que la vida privada se realiza. Por lo que, no se puede intervenir o vigilar comunicaciones a menos que exista un justo motivo y se cumplan estándares de protección a la privacidad como: un debido proceso, una orden judicial, un motivo legítimo, entre otros. La posibilidad de decidir sobre cuestiones privadas: familiares o personales como la de formar una familia, de decidir ser padre biológicos son manifestaciones del libre desarrollo de la personalidad del que todas las personas somos titulares.

Queda entonces, pendiente que la Corte Interamericana use estos criterios jurisprudenciales en el ámbito digital, de manera que, el derecho a la privacidad incluya elementos necesarios para la protección de los derechos humanos en la era digital. Así como ha ocurrido en otros tribunales como el Europeo, que ha ampliado la protección de la correspondencia a las telecomunicaciones y al uso de internet[1049], por ejemplo.

2.3 Recomendaciones de la Organización de Estados Americanos (OEA) sobre protección de datos personales

La Organización de Estados Americanos, OEA se encuentra elaborando una Ley Modelo Interamericana sobre Protección de Datos Personales. Con esta finalidad se convocó a diversos actores del sector público y privado, organizaciones de la sociedad civil, academia, industria, entre otros, para obtener acuerdos mínimos sobre la temática.[1050]

La primera iniciativa en la temática data del 7 de junio de 1996, cuando la Asamblea General de la Organización de los Estados Americanos, mediante la Resolución AG/RES.1395 (XXVI-O/96), solicitó al Comité Jurídico Interamericano (CJI) que al analizar el derecho de la información profundice respecto del acceso y protección de los datos de carácter personal, incluyendo aquellos que se introduzcan vía los sistemas de correo y transmisión electrónica computarizada. [1051]

En noviembre de 2010, se expidió el "Proyecto de principios y recomendaciones preliminares sobre la protección de datos". El trabajo realizado por el Comité Jurídico Interamericano señaló que existen dos sistemas de protección de bases de datos:

[1049] TRIBUNAL EUROPEO DE DERECHOS HUMANOS, Caso Copland c. Reino Unido (Demanda nº 62617/00), Sentencia Estrasburgo 3 abril de 2007, (traducción realizada por Judith Salazar Álvarez), accedido el 2 de noviembre de 2019, https://www.mjusticia.gob.es/cs/Satellite/Portal/1292429139374?Blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Grupo&blobheadervalue1=attachment%3B+filename%3dtrad._Sentencia_COPLAND_c.REINO_UNIDO.pdf&blobheadervalue2=Docs_TEDH

[1050] OEA :: SAJ :: DDI :: PROTECCIÓN DE DATOS PERSONALES, accedido el 2 de noviembre de 2019, http://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo.asp

[1051] *Ibíd.*

> [...] el europeo es hoy el sistema más estricto de regulaciones estatales, con una legislación que rige la recolección de datos personales por el gobierno y las entidades privadas. El sistema de Estados Unidos sigue un criterio bifurcado, que permite que los sectores económicos regulen los datos personales recabados por el Estado. Por último, varios países de América Latina han elaborado mecanismos de protección de datos basados en el concepto de *habeas data*, que permite a las personas acceder a sus propios datos personales y otorga el derecho.

Para el 2011, el Departamento de Derecho Internacional realizó un estudio preliminar que sirvieran para desarrollar un catálogo de principios y recomendaciones que pudieran aplicarse por los Estados miembros. Posteriormente, la Asamblea General, incluyó el tema de protección de datos personales.[1052]

Para el año 2012, el Comité Jurídico Interamericano adoptó y presentó a la Asamblea General los siguientes doce principios que se listan a continuación:

1. Propósitos Legítimos y Justos;
2. Claridad y Consentimiento;
3. Pertinencia y Necesidad;
4. Uso Limitado y Retención;
5. Deber de Confidencialidad;
6. Protección y Seguridad;
7. Fidelidad de la Información;
8. Acceso y Corrección;
9. Información Sensible;
10. Responsabilidad;
11. Flujo Transfronterizo de Información y Responsabilidad; y
12. Publicidad de las Excepciones. [1053]

Por su parte, en los años 2013 y 2014, la Asamblea General resolvió encomendar al Comité Jurídico Interamericano formular propuestas sobre protección de datos personales, y principalmente la elaboración de un *proyecto de Ley Modelo sobre Protección de Datos Personales*.

Para el año 2015, se decidió elaborar una propuesta de Guía Legislativa para los Estados Miembros, basada en los citados doce principios y en las normativas dictadas por la Unión Europea, la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Cooperación Económica Asia-Pacífico (APEC), entre otras. Todo lo anteriormente señalado aparece en el Informe sobre Privacidad y Protección de Datos Personales (CJI/doc. 474/15 rev.2) adoptado por el CJI durante su octogésimo sexto período de sesiones, celebrado del 23 al 27 de marzo de en Río de Janeiro, Brasil.[1054]

A continuación se analizará la Declaración de Principios sobre libertad de expresión de la Comisión Interamericana de Derechos Humanos, primer antecedente de la conceptualización de la privacidad; así como los principales documentos elaborados por el relator David Stewart que figuran como antecedentes de primera iniciativa de

[1052] *Ibíd.*
[1053] *Ibíd.*
[1054] OEA - ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, *Democracia para la paz, la seguridad y el desarrollo, Ley modelo de protección de datos personales*, 2009, accedido 5 de noviembre de 2017, http://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo.asp.

proyecto de Ley Modelo sobre Protección de Datos Personales y la actual versión de Guía Legislativa sobre la citada temática.

2.3.1 Declaración de Principios sobre libertad de expresión de la Comisión Interamericana de Derechos Humanos

La Comisión Interamericana de Derechos Humanos, en octubre de 2000, aprobó la Declaración de Principios sobre Libertad de Expresión durante su 108° período ordinario de sesiones. Mediante este instrumento, se interpreta del artículo 13 de la Convención Americana sobre Derechos Humanos, relativo a la libertad de pensamiento y de expresión.[1055] Esta declaración resulta un hito trascendental, ya que:

> [...] Su aprobación no sólo es un reconocimiento a la importancia de la protección de la libertad de expresión en las Américas sino que además incorpora al sistema interamericano los estándares internacionales para una defensa más efectiva del ejercicio de este derecho.[1056]

A continuación haremos un análisis de aquellos principios relacionados con la privacidad o la protección de los datos personales:

a) Respecto del principio tres de la citada Declaración, este señala que:

> 3. Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla. [1057]

Posteriormente, en el instrumento sobre antecedentes e interpretación de la Declaración de Principios sobre Libertad de Expresión, respecto del citado principio 3, determina que "este principio se refiere a la acción de *habeas data* (12)" [1058]. Es decir, tanto la citada Declaración como su respectiva interpretación reconocen el derecho a la autodeterminación informativa, que en Latinoamérica se concibió originalmente a través de la acción constitucional denominada *habeas data.*

El instrumento de interpretación además aclara que la acción de *habeas data* tiene tres ejes fundamentales:

> […]1) el derecho de cada persona a no ser perturbado en su privacidad, 2) el derecho de toda persona a acceder a información sobre sí misma en bases de

[1055] OEA - ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, *Democracia para la paz, la seguridad y el desarrollo, Antecedentes e Interpretación de la Declaración de Principios de Libertad de Expresión, 2000*, accedido 27 de septiembre de 2018, http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=132&lID=2
[1056] *Ibíd.*
[1057] COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, *Declaración de Principios sobre Libertad de Expresión*, 2000, accedido el 14 de septiembre de 2019, https://www.cidh.oas.org/basicos/declaracion.htm
[1058] *Ibíd.*

> datos públicas y privadas para modificar, anular o rectificar información sobre su persona por tratarse de datos sensibles, falsos, tendenciosos o discriminatorios y 3) el derecho de las personas a utilizar la acción de *habeas data* como mecanismo de fiscalización. Este derecho de acceso y control de datos personales constituye un derecho fundamental en muchos ámbitos de la vida, pues la falta de mecanismos judiciales que permitan la rectificación, actualización o anulación de datos afectaría directamente el derecho a la privacidad, el honor, a la identidad personal, a la propiedad y la fiscalización sobre la recopilación de datos obtenidos. (12) [1059]

El primer eje, hace alusión al *habeas data* como una acción que garantiza la intimidad o privacidad de las personas, postura que ha sido superada con la comprensión de la autodeterminación informativa y el reconocimiento del derecho a la protección de datos personales. En cuanto al segundo eje, hace referencia a lo que se conoce como derechos ARCO, acrónimo de acceso, rectificación, cancelación y oposición; sin embargo limita su implementación al señalar que se refiere a datos sensibles, ya que existen otros datos personales que no entran en esta categoría especial, y que también ameritan protección. Asimismo, en los verbos que definen el campo de acción del *habeas data* no consta la posibilidad de oponerse. Y es que, no es suficiente que solo pueda modificarse o eliminarse un dato cuando este es incorrecto o discriminatorio, sino que basta la simple voluntad del titular del dato, siempre que no exista un motivo legal o legítimo que permita su retención. Finalmente, la tercera caracterización del *habeas data* lo consagra como un mecanismo constitucional que busca la transparencia de una sociedad y la posibilidad de limitar los abusos del poder. Por ello, el citado instrumento de interpretación hace hincapié en el derecho de las personas de usar el *habeas data* como mecanismo de fiscalización para verificar la legalidad de la recopilación de datos de las personas por parte de las agencias de seguridad e inteligencia del Estado; así como permitir al peticionario "conocer la identidad de los involucrados en la recopilación ilegal de datos, habilitando la sanción legal para sus responsables". (14) [1060]

Esta última postura se potencia, cuando se reconoce que debido al avance tecnológico, tanto el Estado como el sector privado obtienen cada vez más información de las personas poniéndolas en riesgo. Por ello, el instrumento de interpretación señala que es indispensable:

> […] garantizar la existencia de canales concretos de acceso rápido a la información para modificar información incorrecta o desactualizada contenida en las bases de datos electrónicas. Asimismo la acción de *habeas data* impone ciertas obligaciones a las entidades que procesan información: el usar los datos para los objetivos específicos y explícitos establecidos; y garantizar la seguridad de los datos contra el acceso accidental, no autorizado o la manipulación. En los casos en que entes del Estado o del sector privado hubieran obtenido datos en forma irregular y/o ilegalmente, el peticionario debe tener acceso a dicha información, inclusive cuando ésta sea de carácter clasificada. (13) [1061]

[1059] *Ibíd.*
[1060] *Ibíd.*
[1061] *Ibíd.*

Desde un orden práctico, este instrumento de interpretación señala que para garantizar la eficiencia de esta figura se requiere "eliminar las trabas administrativas". [1062] Ya que, esta acción, solo surtirá verdaderos efectos, si a través de ella, puede accederse a información personal de forma fácil, simple y a bajos costos. (15) Pero sobre todo, que no se requiera revelar las causas por las cuales se solicita la información. Debido a que la revelación de la motivación del individuo podría afectar otros derechos como su privacidad, su intimidad, su honra o incluso su libertad de pensamiento y de expresión pero además porque "la mera existencia de datos personales en registros públicos o privados es razón suficiente para el ejercicio de este derecho". (16) [1063]

b) En cuanto al principio 10 de la Declaración de Principios de la Libertad de Expresión señala que:

> Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada sólo a través de sanciones civiles, en los casos en que la persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en estos casos, debe probarse que en la difusión de las noticias el comunicador tuvo intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas. [1064]

Este principio propone que el discurso crítico o incluso ofensivo contra quienes ocupan cargos públicos o están íntimamente vinculados a la formulación de la política pública, (42) que no debiera limitarse a través de acciones penales de injuria o calumnia que buscan opacar estas posturas sino que las sanciones deben ser únicamente de carácter civil (45), en aquellos casos en que exista información falsa y producida con "real malicia" (46) En este sentido, la privacidad tampoco debiera usarse como mecanismo para evitar el ejercicio de la libertad de pensamiento o de expresión de un individuo, menos aún permitirse el uso abusivo de sus poderes coactivos para reprimir estas libertades. (45) [1065]

Postura que coincide con el Principio 11 de la Declaración de Principios de la Libertad de Expresión que determina que

> […] los funcionarios públicos están sujetos a un mayor escrutinio por parte de la sociedad. Las leyes que penalizan la expresión ofensiva dirigida a funcionarios públicos generalmente conocidas como "leyes de desacato" atentan contra la libertad de expresión y el derecho a la información.[1066]

De lo visto, podemos colegir que en América Latina, derecho a la libertad de expresión y su relación directa con la privacidad y la intimidad, es antecedente directo del derecho

[1062] *Ibíd.*
[1063] *Ibíd.*
[1064] *Ibíd.*
[1065] *Ibíd.*
[1066] *Ibíd.*

a la protección de datos personales. Ya que, se intenta impedir la injerencia del Estado o de los particulares en la libertad del pensamiento, de opinión y de expresión de las personas. Para lo cual, necesitamos de un espacio de privacidad que nos permita construir nuestro criterio, debatirlo o pronunciarlo en el anonimato e incluso organizarnos y manifestarnos contra el poder.

2.3.2 Privacidad y protección de datos, presentado por el doctor David P. Stewart, el 25 de febrero del 2014

Del 10 al 14 de marzo de 2014, en la ciudad de Río de Janeiro, Brasil, durante el 84° período ordinario de sesiones, la Asamblea General de la OEA encomendó al Comité Jurídico Interamericano para que formule propuestas a la Comisión de Asuntos Jurídicos y Políticos sobre las distintas formas de regular la protección de datos personales, en donde se toma en cuenta los estándares internacionales alcanzados en la materia.

El proyecto de la creación de una ley modelo que trate la protección de datos personales, inicia con la "Propuesta de declaración de principios de privacidad y protección de datos personales en las Américas", siendo la finalidad instar a los Estados a adoptar medidas para que se respete la privacidad, reputación y la dignidad.

Se llevaron a cabo varias medidas como consultas con expertos y otros para la elaboración de principios y prácticas pertinentes, siendo necesario ahondar en el contexto y la creación de la Ley Modelo.

La privacidad personal y la protección de datos están evolucionando constantemente debido a la evolución de la tecnología, por lo que se han elaborado principios guía de la OEA sobre este tema para la preparación e implementación de leyes nacionales y prácticas conexas en los Estados miembros.

Un resultado que podría ser útil sería un volumen para distribuir a los Estados Miembros (gobiernos, legislaturas, expertos, etc.) que contuviera: 1) los Principios de la OEA sobre la privacidad y la protección de datos; 2) una explicación detallada de los asuntos abordados en dichos principios y las consideraciones que deberían tenerse en cuenta al plasmarlos en la legislación interna; y 3) una compilación de instrumentos pertinentes de todo el mundo (entre ellos, por ejemplo, la directiva general de la Unión Europea sobre la protección de datos, los Principios de Madrid, las directrices de la OCDE sobre la protección de la privacidad, el Marco de Privacidad de la APEC, diversas leyes nacionales y "códigos de conducta"). Si de hecho se puede redactar una posible ley modelo, también podría incluirse.

El citado documento señala en su Adjunto A - Borrador interno del Comité Jurídico Interamericano, que la finalidad de la explicación de los principios es proporcionar una guía de preparación e implementación de leyes nacionales y prácticas conexas en los Estados miembros de la OEA. De tal manera que se incorporen reglas efectivas para la protección de derechos fundamentales en la normativa interna de cada país.

Estos principios se aplican tanto para el sector público y el privado; están relacionados entre sí y deben interpretarse en conjunto.

Un acápite especial merecen las definiciones por las cuales: a) el dato personal es toda aquella información sobre una persona identificada o que puede serlo de manera directa e indirecta; b) dato personal sensible, es aquel que afecta los aspectos más íntimos de las personas físicas, merece una protección especial ya que si se divulga o se maneja de manera indebida puede producir grandes prejuicios; c) el titular de los datos, se considera a la persona cuya información se recopila, almacena, utiliza o difunde; d) las personas o entidades encargadas de la información [por determinar]; e) autoridades [por determinar]. [1067]

Asimismo, en cuanto a los Principios constan los siguientes:

1. **Principio 1: Propósitos Legítimos y Justos.** Los datos personales deben de ser recopilados solamente para fines legítimos y por medios justos y legales. Este principio abarca dos elementos: primero, se tiene un requisito de legalidad del fin para el cual se recopilan, retienen y procesan datos personales; esta recopilación debe ser limitada y con conocimiento o consentimiento de la persona; segundo, los medios justos y legales hacen referencia a que la recopilación debe ser compatible con los requisitos jurídicos pertinentes y con las expectativas razonables con el controlador de datos, por lo que los datos no pueden ser obtenidos mediante fraude, engaño, o pretextos falsos.

2. **Principio 2: Claridad y consentimiento.** Este principio también se basa en la recopilación de datos personales; implica la necesidad de que se especifiquen los fines para los cuales se recopilen los datos personales y que se cuente con el consentimiento de la persona a la que se refieren; por lo que debe observarse la transparencia; es decir, existe la obligación de especificar claramente los fines al momento de recopilar dicha información, sin claridad, el consentimiento no es válido, pues este debe basarse en suficiente información. No debe existir duda o ambigüedad respecto de la intención de la persona que recopila; no debe existir riesgo de engaño intimidación o coacción. Este debe ser apropiado para la edad y la capacidad de la persona. El consentimiento debe ir de acuerdo al contexto, pues debe interpretarse de manera razonable en el entorno tecnológico en rápida evolución en el cual se recopilan y usan datos en la actualidad, siendo el momento ideal al momento de realizar la recopilación de los datos.

3. **Principio 3: Pertinencia y necesidad.** Los datos deben ser verídicos, pertinentes y necesarios para los fines expresos de su recopilación. Debe observarse la exactitud, es decir correctos, exactos y completos, siendo necesario evidenciar la calidad de los datos. Además, los datos deben guardar una relación razonable con los fines para los cuales fueron recopilados; la proporcionalidad impone limitaciones generales al uso de dichos datos.

[1067] D. P. STEWART, *Privacidad y Protección de datos No. CJI/doc.450 /14*, Rio de Janeiro, 25 de febrero de 2014, accedido el 2 de noviembre de 2019, http://www.oas.org/es/sla/cji/docs/informes_culminados_recientemente_Proteccion_Datos_Personales_CJI-doc_465-14.pdf

4. **Principio 4: Uso limitado y retención.** Los datos personales deben de ser mantenidos y utilizados solo de manera legítima, no incompatible con el fin o fines para los cuales se recopilaron. No deberán mantenerse más del tiempo necesario para su propósito y de conformidad con la legislación nacional correspondiente. [1068]

En junio de 2014, la Asamblea General de la OEA tomó nota de la resolución del Comité y le encomendó que, la Asamblea General, "formule propuestas a la CAJP sobre las distintas formas de regular la protección de datos personales, incluyendo un proyecto de Ley Modelo sobre Protección de Datos Personales, tomando en cuenta los estándares internacionales alcanzados en la materia". [1069]

El Comité Jurídico Interamericano (agosto de 2013), el Presidente pidió al doctor David P. Stewart que actuara en calidad de relator del tema. [1070] El Relator concluyó que lo mejor sería elaborar una propuesta de guía legislativa para los Estados Miembros. La guía se basaría en los 12 principios adoptados anteriormente por el Comité, con algunas modificaciones menores, teniendo en cuenta directrices de la Unión Europea, la OCDE, APEC, etc. El objetivo era desarrollar los principios, proporcionando un contexto más amplio y orientación a los Estados Miembros a fin de facilitar la elaboración de leyes nacionales.

La respuesta ante la amenaza que representa el abuso de la tecnología ha sido abordada de diferente forma en cada región del mundo. En las Américas se tiene un enfoque "regional" uniforme y coherente, por lo que la intención de este documento es llenar este espacio. Sin embargo, podemos ver que respecto de las iniciativas mundiales como el Reglamento europeo representa un nivel mínimo de protección superado por varias legislaciones locales apegadas al modelo europeo.

2.3.3 Privacy and Data Protection; presentado por David P. Stewart el 28 de julio de 2014

Del 4 al 8 de agosto de 2014, en la ciudad de Río de Janeiro, Brasil, en el 85° Período Ordinario de Sesiones se resolvió realizar un proyecto sobre una Ley Modelo, que contenga principios para la privacidad y protección de datos personales, por lo que se estableció la necesidad de elaborar propuestas basadas en las diferentes formas internacionales en que se protege a los datos personales.

Teniendo en cuenta la necesidad de implementar esta Ley Modelo, se nombró a David P. Stewart como relator sobre este tema.

La creación de estos principios es alentar a que los Estados miembros de la OEA incluyan medidas que aseguren el respeto por la privacidad, la reputación y la dignidad de las personas es decir, el objetivo es servir de base para la formulación y adopción de estos en las legislaciones nacionales.

[1068] *Ibíd.*
[1069] *Ibíd.*
[1070] *Ibíd.*

Para la elaboración de las propuestas se ha contado con la colaboración activa de los gobiernos, expertos, académicos, instituciones gubernamentales y no gubernamentales, entre otros.

Aunque no se ha elaborado un contenido a los principios y la Ley Modelo, se sigue creyendo que este es el mejor camino para incentivar a que los Estados incluyan dentro de las legislaciones principios y reglas que sirvan para la protección de datos personales.

2.3.4 Informe del Comité Jurídico Interamericano, Privacidad y Protección de Datos Personales de 26 de marzo del 2015

Del 23 al 27 de marzo de 2015, en la ciudad de Río de Janeiro, Brasil, en el 86° Período Ordinario de Sesiones, el Comité Jurídico Interamericano adoptó la "Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas"[1071]. La finalidad de estos principios es lograr que los Estados miembros de la organización incluyan dentro de sus legislaciones medidas que respeten la dignidad, privacidad y reputación. Dentro de este informe se incluye una explicación detallada de los mismos que tiene como objetivo el proporcionar una guía para la preparación e implementación de leyes nacionales y normas conexas de los Estados miembros.

En los períodos ordinarios de sesiones anteriores se propuso que se formulen propuestas sobre las distintas formas de regular la protección de datos personales; se encomendó a David Stewart como relator; se pidió a los Estados que informen sobre sus prácticas y leyes vigentes en la materia. De esto se pudo concluir que la orientación más productiva es la elaboración de una guía legislativa que consiste basada en doce principios que proporcionen un contexto más amplio y orientación para los Estados miembros.

Para el relator, la privacidad y la protección de datos evolucionan conforme los avances tecnológicos; los enfoques de protección han sido distintos alrededor del mundo. En América la forma de garantía y protección de estos derechos no es uniforme y coherente; siendo necesario para la elaboración de los principios observar las buenas prácticas de otras regiones del mundo.

La finalidad de los principios de la OEA sobre la privacidad y la protección de datos personales es proteger a las personas de la recopilación, el uso, la retención y divulgación ilícitos o innecesarios de datos personales. Los Estados miembros de la organización debe adoptar e implementar una política clara y eficaz de apertura y transparencia para todos los adelantos, prácticas y políticas con respecto a los datos personales, dejando a discreción de estos la determinación de la mejor manera de implementar estos principios en su ordenamiento jurídico interno.

Las normas nacionales deben asegurar que los datos personales, el derecho de las personas a beneficiarse de la economía digital y los flujos de información que la

[1071] COMITÉ JURÍDICO INTERAMERICANO DE LA OEA, *Informe Privacidad y Protección de Datos Personales No. CJI/doc. 474/15 rev.2*, Rio de Janeiro, 26 de marzo de 2015, accedido el 2 de noviembre de 2019, http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_documentos_referencia_CJI-doc_474-15_rev2.pdf

sustentan deben buscar un equilibrio entre el derecho de las personas a controlar la forma en que se recopilan, almacenan y utilizan sus datos personales y su derecho a tener acceso a los datos; así como los intereses de las organizaciones en el uso de datos personales con fines comerciales legítimos y razonables en una economía basada en datos.

Estos principios se aplican tanto para el sector público y el sector privado, están relacionados entre sí y deben interpretarse en conjunto.

La privacidad se basa en el honor y la dignidad, así como en la libertad de expresión, pensamiento, opinión y asociación. Este no es absoluto y puede tener limitaciones razonables relacionadas de manera racional con metas apropiadas. Conforme consta del anexo A, parte I, derecho de privacidad incluido en la recomendación de 12 principios, el concepto de privacidad está claramente establecido en el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre (1948) y en el artículo 11 de la Convención Americana sobre Derechos Humanos (1969). Únicamente la Carta de los Derechos Fundamentales de la Unión Europea (2000) aborda a la privacidad de manera específica en el contexto de protección de datos.

La sociedad de la información está centrada en la persona y orientada al desarrollo, la protección del derecho de las personas a tener acceso a información y conocimientos, a usarlos y a difundirlos; puedes ayudar a las personas, comunidades y pueblos a alcanzar su pleno potencial, desarrollo y mejorar su calidad de vida. Así aparece el concepto de libre flujo de información.

Respecto de las definiciones, incluye nueva terminología y se precisa otra, como la siguiente: a) Datos personales: consiste en toda información que identifica o puede usarse razonablemente para identificar a una persona en particular de forma directa o indirecta; b) Controlador de datos: es aquella persona física o jurídica, pública o privada, que se encarga del almacenamiento, procesamiento, uso, protección y difusión de datos personales; c) Procesador de datos: persona física o jurídica, pública o privada, que se encarga del conjunto de operaciones realizadas con datos personales, como registro, recopilación, almacenamiento, alteración, recuperación, divulgación o transferencia; d) Autoridad responsable de la protección de datos: en algunos Estados se han establecido organismos reguladores nacionales que se encargan de establecer y hacer cumplir leyes, normas y requisitos relativos a la protección de datos personales; e) Titular de los datos: es la persona cuyos datos personales se recopilan, almacenan, utilizan o difunden; f) Datos personales sensibles: se refiere a una categoría más estrecha que abarca los datos que afectan a los aspectos más íntimos de las personas físicas, estos pueden variar según la cultura o cambiar con el tiempo. [1072]

De lo citado anteriormente, se advierte que por el concepto de datos sensibles se entiende a los datos íntimos según la cultura de cada lugar o tiempo. [1073]

Se desarrollan los doce principios que ahora se conocen como Recomendaciones de Principios de la OEA sobre la protección de la privacidad y los datos personales con anotaciones, cuyo contenido señala lo siguiente:

[1072] *Ibíd.*
[1073] *Ibíd.*

1. **Principio 1: Propósitos legítimos y justos.** Los datos personales deben de ser recopilados solamente para fines legítimos y por medios justos y legales. Este principio abarca dos elementos: primero, se tiene un requisito de legalidad del fin para el cual se recopilan, retienen y procesan datos personales; está recopilación debe ser limitada y con conocimiento o consentimiento de la persona. Segundo, los medios justos y legales hacen referencia a que la recopilación debe ser compatible con los requisitos jurídicos pertinentes y con las expectativas razonables con el controlador de datos, por lo que los datos no pueden ser obtenidos mediante fraude, engaño o pretextos falsos.

2. **Principio 2: Claridad y consentimiento.** Este principio también se basa en la recopilación de datos personales; implica la necesidad de que se especifiquen los fines para los cuales se recopilen los datos personales y que se cuente con el consentimiento de la persona a la que se refieren; por lo que debe observarse la transparencia. Es decir, existe la obligación de especificar claramente los fines al momento de recopilar dicha información; sin claridad, el consentimiento no es válido, pues este debe basarse en suficiente información. No debe existir duda o ambigüedad respecto de la intención de la persona que recopila, no debe existir riesgo de engaño intimidación o coacción, este debe ser apropiado para la edad y la capacidad de la persona. El consentimiento debe ir de acuerdo al contexto, pues debe interpretarse de manera razonable en el entorno tecnológico en rápida evolución en el cual se recopilan y usan datos en la actualidad, siendo el momento ideal al momento de realizar la recopilación de los datos.

3. **Principio 3: Pertinencia y necesidad.** Los datos deben ser verídicos, pertinentes y necesarios para los fines expresos de su recopilación. Debe observarse la exactitud, es decir correctos, exactos y completos, siendo necesario evidenciar la calidad de los datos; además, los datos deben guardar una relación razonable con los fines para los cuales fueron recopilados. La proporcionalidad impone limitaciones generales al uso de dichos datos.

4. **Principio 4: Uso limitado y retención.** Los datos personales deben de ser mantenidos y utilizados solamente de manera legítima, no incompatible con el fin o fines para los cuales se recopilaron. No deberán mantenerse más del tiempo necesario para su propósito y de conformidad con la legislación nacional correspondiente.

5. **Principio 5: Deber de confidencialidad.** Los datos personales no deben divulgarse, ponerse a disposición de terceros, ni emplearse para otros propósitos que no sean aquellos para los cuales se obtuvieron, excepto con el conocimiento o consentimiento de la persona en cuestión o bajo autoridad de la ley.

6. **Principio 6: Protección y seguridad.** Deben ser protegidos mediante salvaguardias razonables y adecuadas contra accesos no autorizados, pérdida, destrucción, uso, modificación o divulgación.

7. **Principio 7: Fidelidad de los datos.** Los datos personales deben mantenerse fieles y actualizados hasta donde sea necesario para los propósitos de su uso.

8. **Principio 8: Acceso y corrección.** Se debe disponer de métodos razonables para permitir que aquellas personas cuyos datos personales han sido recopilados puedan solicitar el acceso a dichos datos y puedan solicitar al controlador de datos que los modifique, corrija o elimine. En caso de que fuera necesario restringir dicho acceso corrección, debería especificarse las razones concretas de cualquiera de estas restricciones de acuerdo con la legislación nacional.

9. **Principio 9: Datos personales sensibles.** Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de

causar daños considerables a las personas si se hace mal uso de ellos. Los controladores de datos deberían adoptar medidas de privacidad y de seguridad que sean acorde con la sensibilidad de los datos y su capacidad de hacer daño a los individuos sujetos de la información.

10. **Principio 10: Responsabilidad.** Los controladores de datos adoptarán e implementarán las medidas correspondientes para el cumplimiento de estos principios.

11. **Principio 11: Flujo transfronterizo de datos y responsabilidad.** Los Estados miembros cooperarán entre sí en la creación de mecanismos y procedimientos que aseguren que los controladores de datos que operen en más de una jurisdicción puedan ser efectivamente hechos responsables por el cumplimiento de estos principios.

12. **Principio 12: Publicidad de las excepciones.** Cuando las autoridades nacionales establezcan excepciones a estos principios por motivos relacionados con la soberanía nacional, la seguridad interna o externa, el combate con la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, deberían poner en conocimiento del público dichas excepciones. [1074]

Estos principios son fruto de una construcción que recoge la tendencia internacional basado en los principales instrumentos internacionales que han citado alguna postura sobre de la defensa de los derechos fundamentales, en especial la intimidad y el *habeas data*. De este modo:

> [...] esta compatibilidad se hace visible frente al Sistema Universal de Protección de Derechos Humanos, así como frente al Sistema Interamericano, a través de instrumentos como la Observación General No. 16, interpretativa del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y otros, como el Informe Anual de la Relatoría para la Libertad de expresión CIDH o los preparativos para el Proyecto de principios y recomendaciones preliminares sobre la protección de datos.[1075]

Finalmente, en el anexo A del documento en análisis consta en la parte III, los apéndices sobre la privacidad y protección de datos en los que se encuentran:

- Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales (1980, revisión de 2013)
- La Resolución de Madrid: Estándares internacionales sobre protección de datos personales y privacidad (2009)
- Marco de Privacidad de APEC (2004)
- Sistema de reglas de privacidad transfronteriza de APEC
- Directiva 2002/58/EC del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas (12 de julio de 2002)
- Directiva 95/46/EC del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (24 de octubre de 1995)

[1074] *Ibíd.*
[1075] TERCERA DE REVISIÓN DE LA CORTE CONSTITUCIONAL DE COLOMBIA, *Sentencia T-058_2015*, p. 58, fecha de consulta 26 mayo 2018, en http://www.cancilleria.gov.co/sites/default/files/Normograma/docs/t-058_2015.htm.

- Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (No. 108, 28 de enero de 1981) y su Protocolo (2001)
- Principios rectores de las Naciones Unidas para la reglamentación de los ficheros computarizados de datos personales (1990)
- Convenio de la Unión Africana sobre ciberseguridad y datos personales (adoptado el 27 de junio de 2014)

La finalidad de los Principios de la OEA sobre la privacidad y la protección de datos personales es establecer un marco para salvaguardar los derechos de la persona a la protección de los datos personales y a la autodeterminación en lo que respecta a la información. Los principios se basan en normas reconocidas a nivel internacional.

Cada Estado Miembro de la OEA debe adoptar e implementar una política clara y eficaz de apertura y transparencia para todos los adelantos, prácticas y políticas con respecto a los datos personales.

Las normas nacionales deben asegurar que los datos personales se recopilen únicamente con fines legítimos y se procesen de una manera justa, legal y no discriminatoria. Es decir, que se recopilan, procesan, usan y difunden de forma apropiada y con el debido respeto de los derechos de la persona. Además que, el titular reciba información sobre la identidad de las personas o entidades que recopilan datos, los fines para los cuales se recopilan, los mecanismos de protección conferidos a las personas y las formas en que las personas pueden ejercer esos derechos.

Al mismo tiempo, la normativa nacional debe proteger el derecho de las personas a beneficiarse de la economía digital y los flujos de información que la sustentan. De tal forma que, permita a consumidores y empresas beneficiarse del uso de datos personales de una manera segura y protegida.

Debe existir una neutralidad tecnológica que faculte el libre flujo de datos dentro de cada país y a través de las fronteras nacionales de una manera que fomente la innovación tecnológica y promueva el desarrollo económico y el crecimiento del comercio.

Sin duda, esta iniciativa es valiosa para la región y el mundo, pues de haberse concluido con la elaboración de la Ley Modelo, contaríamos con un instrumento clave como Guía Legislativa que identifique el contenido esencial de este derecho para su efectiva protección. Los Estados podrían ofrecer mecanismos de protección adicionales para la privacidad de los datos personales. Los citados principios reflejan la importancia de la efectividad, la razonabilidad, la proporcionalidad y la flexibilidad como elementos rectores.[1076]

Sin embargo, este proyecto no ha logrado trascender tanto más que en el continente europeo se ha superado la visión de una ley modelo y se ha previsto una normativa comunitaria de carácter vinculante como el Reglamento Europeo. Esto se debe no solo a que se logra una homologación legislativa, una univocidad de interpretación y

[1076] COMITÉ JURÍDICO INTERAMERICANO DE LA OEA, *Informe Privacidad y Protección de Datos Personales No. CJI/doc. 474/15 rev.2*

aplicación, sino que es parte de una estrategia comunitaria que permite que los Estados en su conjunto puedan contrarrestar a las grandes plataformas y corporaciones que manejan datos personales, las que incluso están por fuera del territorio europeo. Así, ahora mismo el documento que marca las directrices o el estándar sobre el glosario, ámbito, objeto, objetivos, principios, derechos, autoridades, entre otros, es el citado Reglamento Europeo de Protección de Datos Personales.

2.4 Recomendaciones de las Naciones Unidas sobre protección de datos personales

2.4.1 Resolución 45/95 sobre las directrices para la regulación de los archivos de datos personales informatizados, de 14 de diciembre de 1990.

Conforme la Resolución 45/95 de la Asamblea General de las Naciones Unidas sobre las directrices para la regulación de los archivos de datos personales informatizados, de 14 de diciembre de 1990[1077], cada Estado podrá seguir en sus legislaciones, bajo su propia iniciativa, las siguientes orientaciones respecto de los procedimientos para llevar a la práctica los principios acerca de las garantías mínimas relativas a los archivos de datos personales informatizados:

1) Principio de legalidad y lealtad

> La información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales, ni debe ser utilizada para fines contrarios a los fines y principios de la Carta de Naciones Unidas.[1078]

Es decir, deben ser usados para favorecer el cumplimiento y respeto de los derechos fundamentales.

2) Principio de exactitud

> Las personas responsables de la compilación de archivos, o aquellas responsables de mantenerlos, tienen la obligación de llevar a cabo comprobaciones periódicas acerca de la exactitud y pertinencia de los datos registrados y garantizar que los mismos se mantengan de la forma más completa posible, con el fin de evitar errores de omisión, así como de actualizarlos periódicamente o cuando se use la información contenida en un archivo, mientras están siendo procesados.[1079]

Este contenido se refiere a lo que la doctrina y legislación específica denominan principio de calidad, por el cual se establece una obligación de cuidado y verificación de la actualización, completitud, corrección y exactitud de la información personal recopilada.

3) Principio de especificación de la finalidad

[1077] ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Resolución 45/95 sobre las directrices para la regulación de los archivos de datos personales informatizados*, 1990, accedido el 12 de agosto de 2019, https://www.un.org/es/documents/ag/res/45/list45.htm

[1078] *Ibíd.*

[1079] *Ibíd.*

> La finalidad a la que vaya a servir un archivo y su utilización en términos de dicha finalidad debe ser especificada, legítima y, una vez establecida, recibir una determinada cantidad de publicidad o ser puesta en conocimiento de la persona interesada, con el fin de que posteriormente sea posible garantizar que: a) Todos los datos personales recogidos y registrados sigan siendo pertinentes y adecuados para los fines especificados; b) Ninguno de los referidos datos personales sea utilizado o revelado, salvo con el consentimiento de la persona afectada, para fines incompatibles con aquellos especificados; c) El período durante el que se guarden los datos personales no supere aquel que permita la consecución de los fines especificados. [1080]

La finalidad como principio tiene diversos enfoques que han sido incorporados en varias legislaciones latinoamericanas como: el deber de información y derecho de información; compatibilidad de la finalidad con lo informado en su recogida, verificación de la pertinencia y adecuación a la finalidad y su legitimidad.

Ahora bien, existen otros enfoques que debieran ser tomados en cuenta y que constan descritos en estas recomendaciones de la ONU referidas a: la imposibilidad de levantar la confidencialidad para fines incompatibles y sin autorización del titular y la mención sobre la temporalidad de la permanencia de los datos en relación a sus fines.

Asimismo, varias normativas latinoamericanas han relevado otros criterios de protección de la finalidad como es la relativa a la cesión de datos, al de *habeas data* y al bloqueo, cancelación y actualización como derechos propios de los titulares de los datos, tal como se analizó en el acápite pertinente.

4) Principio de acceso de la persona interesada

> Cualquiera que ofrezca prueba de su identidad tiene derecho a saber si está siendo procesada información que le concierna y a obtenerla de forma inteligible, sin costes o retrasos indebidos; y a conseguir que se realicen las rectificaciones o supresiones procedentes en caso de anotaciones ilegales, innecesarias o inexactas, y, cuando sea comunicada, a ser informado de sus destinatarios. Debe preverse un recurso, en caso necesario, ante la autoridad supervisora especificada más abajo en el principio 8. El coste de cualquier rectificación será soportado por la persona responsable del archivo. Es conveniente que las disposiciones relacionadas con este principio se apliquen a todas las personas, sea cual sea su nacionalidad o lugar de residencia. [1081]

En este principio se encuentran incluidos tres derechos que se manejan en la doctrina y en varias legislaciones latinoamericanas: derecho de acceso, derecho de rectificación y derecho de cesión. Todos estos derechos tienen el objetivo de devolverle al titular del dato, la posibilidad de decidir sobre su tratamiento. Llama la atención que este principio parte desde la perspectiva de que las personas deben probar la identidad de cualquier manera, por lo que para 1990 la ONU comprendía los datos personales desde una perspectiva de identidad. Pero, además, requerían de un tema probatorio aunque de la redacción se amplía a que puede probarse de cualquier forma.

5) Principio de no discriminación

[1080] *Ibíd.*
[1081] *Ibíd.*

> Sin perjuicio de los casos susceptibles de excepción restrictivamente contemplados en el principio 6, no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato. [1082]

No se ha incorporado en las normativas latinoamericanas la perspectiva de principio de no discriminación, sino que se ha previsto un nivel de protección reforzada para aquellos casos en los que se recolecta datos personales sensibles, que justamente son aquellos que por su naturaleza pueden dar pie a discriminaciones por referirse a cuestiones muy íntimas de las personas que pueden llevar a categorizarlas.

6) Facultad para hacer excepciones

> Las excepciones a los principios 1 a 4 solamente pueden ser autorizadas en caso de que sean necesarias para proteger la seguridad nacional, el orden público, la salud pública o la moralidad, así como, entre otras cosas, los derechos y libertades de otros, especialmente de personas que estén perseguidas (cláusula humanitaria), siempre que tales excepciones estén especificadas de forma explícita en una ley o norma equivalente promulgada de acuerdo con el sistema jurídico interno, que expresamente establezca sus límites y prevea las salvaguardas adecuadas. Las excepciones al principio 5, relativo a la prohibición de la discriminación, además de estar sujetas a las mismas salvaguardas que las prescritas para las excepciones a los principios 1 a 4, solamente podrán autorizarse dentro de los límites establecidos en la Carta Internacional de Derechos Humanos y en el resto de instrumentos aplicables en el campo de la protección de los derechos humanos y la prevención de la discriminación. [1083]

Conforme la recomendación, se puede establecer excepciones a los principios de legalidad y lealtad y de acceso a la persona interesada para cuestiones de interés general como son la seguridad nacional, el orden público, la salud pública así como para el cumplimiento de los derechos humanos de personas que pudieran ser víctimas de persecución. Ahora bien, estas excepciones no se han manejado en la normativa latinoamericana desde la perspectiva de excepciones a la legalidad y lealtad, sino desde la perspectiva de que será la ley la que autorice la recogida de este tipo de información como una forma de salvaguarda que debe realizar el legislador. Ya que, será este el que deberá realizar el *test* de proporcionalidad y verificar si la recolección de un dato personal sin consentimiento del titular debe realizar y por ende ser autorizada legalmente, en virtud de que el bienestar general, el interés común o los beneficios generales o minimización de riesgos son suficientes para que se justifique la recolección o la no eliminación o utilización de estos datos personales.

7) Principio de seguridad

> Deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, como la pérdida o destrucción accidental, como humanos, como el acceso no autorizado, el uso fraudulento de los datos o la contaminación mediante virus informáticos. [1084]

[1082] *Ibíd.*
[1083] *Ibíd.*
[1084] *Ibíd.*

Este principio es recogido en la mayoría de legislaciones latinoamericanas, incluso en aquellas que protegen los datos personales desde la perspectiva acotada de la intimidad. La normativa incluye los distintos ámbitos de seguridad, esto es: física, operativa, funcional y tecnológica.

8) Supervisión y sanciones

> El derecho de cada país designará a la autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios arriba establecidos. Esta autoridad ofrecerá garantías de imparcialidad, independencia frente a las personas o agencias responsables de procesar y establecer los datos, y competencia técnica. En caso de violación de lo dispuesto en la ley nacional que lleve a la práctica los principios anteriormente mencionados, deben contemplarse condenas penales u otras sanciones, junto con los recursos individuales adecuados. [1085]

Esta recomendación es fundamental para que se pueda garantizar un cumplimiento real de la normativa de protección de datos, ya que solo la independencia, la imparcialidad puede generar garantías suficientes que permitan la no intromisión de entes privados o de las propias intervenciones estatales.

En este sentido, llama la atención que legislaciones como la colombiana y la peruana, cuyos países son parte de la ONU, no hayan incorporado en sus legislaciones este principio fundamental, ya que las respectivas entidades de control están inmersas en el Ejecutivo, como en el caso peruano, o la competencia sobre la protección de los datos personales está atribuida a la Superintendencia de Industria y Comercio (SIC), entidad que tiene una orientación diferente a la protección de derechos.

9) Flujo transfronterizo de datos

> Cuando la legislación de dos o más países afectados por un flujo transfronterizo de datos ofrezca salvaguardas similares para la protección de la intimidad, la información debe poder circular tan libremente como dentro de cada uno de los territorios afectados. En caso de que no existan salvaguardas recíprocas, no deberán imponerse limitaciones indebidas a tal circulación, sino solamente en la medida en que lo exija la protección de la intimidad. [1086]

De la lectura de este principio se colige que la protección de los datos que realizó la ONU para el año 1990 era desde la perspectiva generalizada aplicaba en aquel entonces, esto es el derecho a la intimidad. Propuesta ampliamente superada en la actualidad. Sin embargo, nos da luces sobre la problemática del flujo transfronterizo porque establece como primer elemento la reciprocidad que ahora, si bien se garantiza el libre flujo, se lo hace desde la perspectiva de nivel adecuado de protección por tratarse de un sistema de protección de derechos fundamentales del individuo, más que de mecanismos de cooperación entre países.

10) Campo de aplicación

> Los presentes principios deben hacerse aplicables, en primer lugar, a todos los archivos informatizados públicos y privados, así como, mediante extensión optativa y sujeta a los

[1085] *Ibíd.*
[1086] *Ibíd.*

> ajustes correspondientes, a los archivos manuales. Pueden dictarse disposiciones especiales, también optativas, para hacer aplicable la totalidad o parte de los principios a los archivos relativos a personas jurídicas, especialmente cuando contengan alguna información relativa a individuos. [1087]

Este principio aclara muchos de los criterios básicos del contenido esencial, respecto del ámbito de aplicación, esto es: los datos personales se entienden aquellos automatizados o informatizados como manuales; los titulares son personas naturales en primer momento y personas jurídicas, especialmente si contienen información de personas físicas. Finalmente, el ámbito está tanto para bases de datos públicas como privadas, es decir, tanto aquellas regentadas por los particulares como por el Estado.

B. Aplicación de las directrices a archivos de datos personales mantenidos por organizaciones internacionales gubernamentales

> Las presentes directrices serán de aplicación a los archivos de datos personales que mantengan las organizaciones internacionales gubernamentales, sujetas a cualquier ajuste que sea preciso para tener en cuenta cualquier diferencia que pueda existir entre archivos para fines internos, como aquellos que conciernen a la gestión de personal, y archivos para fines externos, relativos a terceros que tengan relaciones con la organización. Cada organización debe designar a la autoridad legalmente competente para supervisar la observancia de estas directrices. Cláusula humanitaria: puede preverse específicamente una excepción a estos principios cuando la finalidad del archivo sea la protección de los derechos humanos y las libertades fundamentales de la persona afectada, o la ayuda humanitaria. Debe preverse una excepción similar en la legislación nacional para las organizaciones internacionales gubernamentales cuyo acuerdo organizativo no impida la puesta en práctica de la referida legislación nacional, así como para las organizaciones internacionales no gubernamentales a las que sea aplicable esta ley. [1088]

Esta norma permite clarificar la aplicación de estas directrices y sus correspondientes principios a organizaciones internacionales gubernamentales, incluidas aquellas que recogen o tratan datos en búsqueda de proteger derechos humanos y libertades fundamentales.

2.4.2 Resolución 26/13 sobre promoción, protección y disfrute de los derechos humanos en Internet, de 29 de junio de 2012

En resolución 26/13 del Consejo de Derechos Humanos de 26 de junio de 2012[1089] se ha determinado la promoción, protección y disfrute de los derechos humanos en Internet al tenor de lo siguiente:

> 1. Afirma que los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la

[1087] *Ibíd.*
[1088] *Ibíd.*
[1089] CONSEJO DE DERECHOS HUMANOS DE LAS NACIONES UNIDAS, *Resolución No. 26/13 sobre Promoción, protección y disfrute de los derechos humanos en Internet*, 2013, accedido el 12 de agosto de 2019, https://www.civilisac.org/civilis/wp-content/uploads/Resolucion-internet.pdf

> Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos;
> 2. Reconoce la naturaleza mundial y abierta de Internet como fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas; […]
> 5. Decide seguir examinando la promoción, la protección y el disfrute de los derechos humanos, incluido el derecho a la libertad de expresión, en Internet y en otras tecnologías, así como la forma en que Internet puede ser un importante instrumento para el desarrollo y para el ejercicio de los derechos humanos, de conformidad con su programa de trabajo. [1090]

De lo citado, el Internet es un adelanto tecnológico que debe propiciar una mejor calidad de vida del individuo. Para que esto sea posible es necesario que los derechos humanos puedan ser protegidos en estos entornos tecnológicos. De ahí que se está evidenciando la necesidad de analizar estas nuevas facetas o enfoques digitales para completar y añadir nuevas características, condiciones o elementos esenciales a los derechos existentes. Pero además, debemos comprender que aparecerán otros derechos que tienen su origen directo en el desarrollo tecnológico y que irán completando el catálogo de derechos digitales del que ahora las personas gozamos en garantía de que nuestra dignidad ya no es solo física sino virtual y que es indispensable una protección integral.

2.4.3 Resolución 69/166 sobre el Derecho a la Privacidad en la Era Digital, de 18 de diciembre de 2014

La Asamblea General de las Naciones Unidas, el 18 de diciembre de 2014, dictó la Resolución *69/166* sobre el Derecho a la Privacidad en la Era Digital,[1091] aprobada, entre otros, por 12 países latinoamericanos: Alemania, Argentina, Austria, Bolivia (Estado Plurinacional de), Brasil, Chile, Cuba, Ecuador, Eslovenia, España, Francia, Guatemala, Indonesia, Irlanda, Liechtenstein, Luxemburgo, México, Nicaragua, Perú, República Popular Democrática de Corea, Suiza, Timor-Leste y Uruguay.

Dicho documento tiene por finalidad reafirmar los derechos de las personas, en especial el derecho a la privacidad en el entorno digital, y hace referencia a la Resolución 68/167 de la ONU sobre el derecho a la privacidad en la era digital de 18 de diciembre de 2013 y al informe A/HRC/23/40 del relator especial Frank de la Rué sobre la promoción y protección del derecho a la libertad de opinión y de expresión, presentado ante el Consejo de Derechos Humanos en el 23º período de sesiones. Ahí se manifestaba la preocupación por las implicaciones de la vigilancia e interceptación extraterritoriales de las comunicaciones realizadas por varios Estados que podrían poner en riesgo el ejercicio de los derechos humanos a la privacidad y a la libertad de opinión y expresión.

En contexto, estos documentos son la respuesta a las noticias sobre la vigilancia y monitoreo de las comunicaciones en distintos países dadas a conocer por Edward Snowden.

Dicha resolución exhorta a los Estados miembros de las Naciones Unidas a que:

[1090] Ibíd.

[1091] ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Resolución 69/166 sobre el Derecho a la Privacidad en la Era Digital*, 2014, accedido el 12 de agosto de 2019, https://undocs.org/es/A/RES/69/166

> a) Respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales;
> b) Adopten medidas para poner fin a las violaciones de esos derechos y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos;
> c) Examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo de todas sus obligaciones en virtud del derecho internacional de los derechos humanos;
> d) Establezcan o mantengan mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado.
> e) Proporcionen acceso a un recurso efectivo a las personas cuyo derecho a la privacidad haya sido violado mediante la vigilancia ilícita o arbitraria, de conformidad con las obligaciones internacionales en materia de derechos humanos.[1092]

Esta resolución tiene una perspectiva limitada debido a que se encuentra atada a la privacidad e intimidad y no reconoce al derecho a la protección de datos personales. Por eso, solicita se proteja las comunicaciones digitales para precautelar la privacidad de las personas. Es decir, no se protegen los datos personales por la sola condición de tales. Además, se alude a la seguridad, respecto de la vigilancia e interceptación de las comunicaciones y recopilación de datos personales, pero nuevamente desde el enfoque de privacidad.

Si bien Ecuador es uno de los países firmantes de los compromisos transcritos, pese a tener una Constitución que reconoce no solo el derecho a la intimidad sino el derecho a la protección de datos personales, cada uno con su propio contenido esencial; no obstante, no ha logrado dictar una ley especializada, sino únicamente dictar normativas sectoriales que no logran responder a los niveles de protección que deben instaurarse, que en el caso ecuatoriano no pueden limitarse a la visión reducida de protección basada en la privacidad.

De la citada resolución, la recomendación más importante radica en aquella que señala que los países firmantes, entre ellos, Ecuador, al dictar la normativa pertinente debe establecer medidas de protección de las comunicaciones y recopilación de datos que pudieran afectar la privacidad y la libertad de expresión; procedimientos y mecanismos de supervisión independientes que prevengan, orienten y controlen posibles transgresiones, por lo que la necesidad de un órgano independiente, más aún con la realidad histórica de nuestros países resulta primordial.

2.4.4 Resolución 69/204 sobre tecnologías de la información y las comunicaciones para el desarrollo, de 18 de diciembre de 2014

La Resolución 69/204 sobre tecnologías de la información y las comunicaciones para el desarrollo, aprobada por la Asamblea General de Naciones Unidas, el 19 de diciembre

[1092] Ibíd.

de 2014[1093], reconoce el valor sustancial, en toda sociedad democrática, de las tecnologías de la información y comunicación, ya que:

> […] tienen el potencial de brindar nuevas soluciones a los problemas del desarrollo, en particular en el contexto de la globalización, y pueden promover el crecimiento económico sostenido, inclusivo y equitativo y el desarrollo sostenible, la competitividad, el acceso a la información y los conocimientos, la erradicación de la pobreza y la inclusión social, factores que contribuirán a acelerar la integración en la economía global de todos los países, especialmente los países en desarrollo y en particular los países menos adelantados;[…] [1094]

Asimismo, reconoce a las tecnologías de la información y la comunicación como elemento clave y catalizador del cumplimiento de los objetivos del Desarrollo del Milenio (18) y como mecanismo que permite superar la brecha digital.(22)

2.4.5 Resolución 28/16 sobre el derecho a la privacidad en la era digital, de 1 de abril de 2015

La Resolución 28/16 sobre el derecho a la privacidad en la era digital, de 1 de abril de 20151095, aprobada por el Consejo de Derechos Humanos recoge lo señalado por la Resolución 69/166 de 2014 y adicionalmente realiza las siguientes recomendaciones:

Determina la importancia de la privacidad en la época actual, en tal sentido, por primera vez, "[A]firma que los derechos de las personas, incluido el derecho a la privacidad, también deben estar protegidos en Internet". ***1096*** Pero además, crea la Relatoría Especial sobre el derecho a la privacidad y nombra su titular por un período de tres años. Entre las principales funciones del citado Relator Especial están las siguientes:

> […] a) Reunir información pertinente, entre otras cosas sobre los marcos internacionales y nacionales y las prácticas y la experiencia nacionales, estudiar las tendencias, las novedades y los retos relacionados con el derecho a la privacidad, y formular recomendaciones para garantizar su promoción y protección, en particular en relación con los retos que plantean las nuevas tecnologías;
>
> b) Buscar, recibir y responder a información, evitando duplicaciones, de los Estados, las Naciones Unidas y sus organismos, programas y fondos, los mecanismos regionales de derechos humanos, las instituciones nacionales de derechos humanos, las organizaciones de la sociedad civil, el sector privado, incluidas las empresas comerciales, y otros interesados o partes pertinentes;
>
> c) Determinar posibles obstáculos a la promoción y protección del derecho a la privacidad, determinar, intercambiar y promover principios y mejores prácticas a nivel nacional, regional e internacional, y presentar propuestas y

[1093] ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Resolución 69/204 sobre tecnologías de la información y las comunicaciones para el desarrollo*, 2014, accedido el 29 de agosto de 2019, https://unctad.org/es/PublicationsLibrary/ares69d204_es.pdf
[1094] Ibíd.
[1095] ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Resolución 28/16 sobre el derecho a la privacidad en la era digital*, 2015, accedido el 29 de agosto de 2019, http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=dtYoAzPhJ4NMy4Lu1TOebIM8c1X4GZjGEGHV9SBM9XSLrkyhn8X9OP5PErl472DFS0WGHKjiDqlMTqWwtmsbg%2B0%2FwzDfM6vlTrrWIR7iAZGazm7af2xJyOwQ13wo5CrT
[1096] Ibíd.

> recomendaciones al Consejo de Derechos Humanos a ese respecto, entre otras cosas en relación con retos concretos de la era digital; […]
>
> e) Concienciar acerca de la importancia de promover y proteger el derecho a la privacidad, entre otras cosas en relación con retos concretos de la era digital, así como acerca de la importancia de proporcionar a las personas cuyo derecho a la privacidad haya sido vulnerado un recurso efectivo acorde con las obligaciones internacionales de derechos humanos;
>
> f) Integrar una perspectiva de género en todas las actividades del mandato;
>
> g) Denunciar las presuntas violaciones, dondequiera que tengan lugar, del derecho a la privacidad establecido en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, en particular en relación con los retos que plantean las nuevas tecnologías, y poner en conocimiento del Consejo y del Alto Comisionado de las Naciones Unidas para los Derechos Humanos las situaciones de especial gravedad;
>
> h) Presentar un informe anual al Consejo de Derechos Humanos y a la Asamblea General, a partir de sus períodos de sesiones 31º y septuagésimo primero, respectivamente. […] [1097]

De las funciones citadas, llama la atención la relativa a la obligación de denunciar ante el Consejo y el Alto Comisionado de las Naciones Unidas las transgresiones graves a la privacidad, ya que a través de este mecanismo se pretende identificar e impedir que se generalicen estas violaciones, lo que concuerda con la función de afrontar aquello casos concretos, en especial los relacionados con la implementación de nuevas tecnologías cuyas consecuencias aún no se avizoran. De esta manera, el Relator especial no solo cumple un rol de armonizador de las normas para permitir un sistema homologado de protección de la privacidad en el mundo, sino se convierte en un vigía que debe anticiparse a impedir, de ser posible, nuevas formas de vulneración o en su caso, la masificación de las trasgresiones o daños, a través de alertas que puedan propiciar pronunciamientos, por parte de estos altos organismos mundiales.

2.4.6 Resolución 70/01 sobre transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible, ODS, de 25 de septiembre de 2015

Resolución 70/01 sobre transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible aprobada por la Asamblea General de Naciones Unidas el 25 de septiembre de 2015.[1098]

Esta resolución establece un plan de acción:

> […] en favor de las personas, el planeta y la prosperidad. También tiene por objeto fortalecer la paz universal dentro de un concepto más amplio de la libertad. Reconocemos que la erradicación de la pobreza en todas sus formas y dimensiones,

[1097] *Ibíd.*
[1098] ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Resolución 70/01 sobre transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible*, 2015, accedido el 29 de agosto de 2019, https://unctad.org/meetings/es/SessionalDocuments/ares70d1_es.pdf

> incluida la pobreza extrema, es el mayor desafío a que se enfrenta el mundo y constituye un requisito indispensable para el desarrollo sostenible.[1099]

En este sentido, dicha resolución establece la importancia de respetar, proteger y promover, sin discriminación alguna, los derechos que constan de la Declaración Universal de Derechos Humanos. Con especial énfasis en la lucha por la igualdad entre los géneros y el empoderamiento de mujeres y niñas.

Además, se reconoce que a través de la globalización de las Tic y de la interconexión e interoperabilidad mundial se puede acelerar el progreso humano, pues se superar la brecha digital y se desarrollan sociedades del conocimiento y de la innovación científica y tecnológica.

Los objetivos planteados en este plan de acción que apuntalan al desarrollo tecnológico son:

a) *Objetivo 4: R*elativo a "Garantizar una educación inclusiva y equitativa de calidad y promover oportunidades de aprendizaje permanente para todos" [1100], por el cual se pretende apoyar a estudiantes para ingresar a programas de enseñanza superior con énfasis en programas técnicos, científicos, de ingeniería y de tecnología de la información y comunicaciones.
b) *Objetivo 5:* Sobre "Lograr la igualdad de género y empoderar a todas las mujeres y las niñas" [1101], para lo cual se pretende mejorar el uso de las TIC para promover el empoderamiento de las mujeres.
c) *Objetivo 9*: Relativo a "Construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación" [1102], por el cual se busca el incremento significativo del acceso universal y asequible a Internet, a las TIC y se promueva el desarrollo de tecnologías, de investigación y de innovación nacionales en los países en desarrollo, a través de normas que, al menos, propicien la diversificación industrial y la adición de valor a los productos básicos. Todo ello con la visión mundial de "mejorar la coordinación entre los mecanismos existentes, en particular a nivel de las Naciones Unidas, y mediante un mecanismo mundial de facilitación de la tecnología".[1103]

Sin duda, esta resolución resulta trascendente para el planeta porque enfoca los esfuerzos mundiales en aquellos objetivos que garantizan paz, igualdad y equidad económica y social. En tal sentido, la tecnología es una herramienta que, adecuadamente utilizada, viabiliza este propósito. Por ello, es indispensable que se garanticen el respeto de los derechos humanos, en línea y fuera de ella, pues solo de esta forma se podrá cumplir con el objetivo principal que es el respeto y la promoción de la dignidad humana.

[1099] *Ibíd.*
[1100] *Ibíd.*
[1101] *Ibíd.*
[1102] *Ibíd.*
[1103] *Ibíd.*

2.4.7 Resolución 70/125, sobre el documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información, de 16 de diciembre de 2015.

La resolución 70/125, sobre el documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información aprobada por la Asamblea General el 16 de diciembre de 2015[1104], determina lo siguiente:

> 44. Sin embargo, observamos con preocupación que existen amenazas graves a la libertad de expresión y la pluralidad de la información, y hacemos un llamamiento a la protección de los periodistas, los trabajadores de los medios de comunicación, y el espacio de la sociedad civil. Pedimos a los Estados que adopten todas las medidas necesarias para garantizar el derecho a la libertad de opinión y de expresión, el derecho de reunión y asociación pacíficas, y el derecho a no ser objeto de injerencias arbitrarias o ilícitas en la vida privada, de conformidad con sus obligaciones en materia de derechos humanos.
> 46. Recordamos la resolución 69/166 de la Asamblea General, y en este contexto recalcamos que nadie será objeto de injerencias arbitrarias o ilícitas en su vida privada, su familia, su domicilio o su correspondencia, en consonancia con las obligaciones que incumben a los países en virtud del derecho internacional de los derechos humanos. En consecuencia, exhortamos a todos los Estados a que revisen sus procedimientos, prácticas y legislación sobre vigilancia de las comunicaciones, así como su interceptación, y la reunión de datos personales, incluida la vigilancia en gran escala, con miras a afianzar el derecho a la privacidad, establecido en la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos para los Estados que son parte en el Pacto, asegurando la aplicación plena y efectiva de todas las obligaciones que les incumben en virtud del derecho internacional de los derechos humanos. [1105]

Estos documentos emitidos por las Naciones Unidas reconocen el riesgo que plantea Internet al ejercicio de los derechos humanos en especial a la libertad de expresión y a la vida privada. Debe recalcarse la referencia a la vigilancia a gran escala a través de la compilación de datos personales, ya que pasa a ser parte de las preocupaciones esta nueva forma de transgresión y por ende la necesidad de diferenciarla de otras formas de vulneración asociadas exclusivamente a la vigilancia de comunicación e interceptación. En suma el derecho internacional de los derechos humanos, ahora más que nunca, cobra importancia debido a que las transgresiones son globales y transnacionales.

2.4.8 Resolución 32/13 sobre promoción, protección y disfrute de los derechos humanos en Internet, de 1 de julio de 2016

La Resolución 32/13 sobre promoción, protección y disfrute de los derechos humanos en Internet, de 1 de julio de 2016[1106], aprobada por el Consejo de Derechos Humanos,

[1104] *Ibíd.*
[1105] Ibíd.
[1106] CONSEJO DE DERECHOS HUMANOS DE LAS NACIONES UNIDAS, *Resolución 32/13 sobre promoción, protección y disfrute de los derechos humanos en Internet*, 2016, accedido el 29 de agosto de 2019, | https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/156/93/PDF/G1615693.pdf?OpenElement

señala que Internet, usado como canal de comunicaciones, puede ser un espacio en el que se transgredan derechos humanos, por ello:

> […] 9. Condena inequívocamente todos los abusos y violaciones de los derechos humanos, como torturas, ejecuciones extrajudiciales, desapariciones forzadas y detenciones arbitrarias, así como la expulsión, intimidación y hostigamiento y la violencia de género cometida contra las personas por ejercer sus derechos humanos y libertades fundamentales en Internet, y exhorta a todos los Estados a que garanticen la rendición de cuentas a este respecto;
>
> 10. También condena inequívocamente las medidas cuyo objetivo deliberado es impedir u obstaculizar el acceso o la divulgación de información en línea, vulnerando el derecho internacional de los derechos humanos, y exhorta a todos los Estados a que se abstengan de adoptar estas medidas, o cesen de aplicarlas;
>
> 11. Destaca la importancia de luchar contra la apología del odio, que constituye una incitación a la discriminación y la violencia en Internet, entre otras cosas fomentando la tolerancia y el diálogo; […][1107]

Esta exhortación recomienda a los países a no imponer medidas restrictivas de acceso a la información (neutralidad en la red), así como realizar acciones positivas que impidan la transgresión de derechos en Internet, con especial énfasis en la protección de la vida, la lucha de género y los discursos de odio. Este instrumento es importante, en la medida que reconoce, que las trasgresiones producidas en el mundo en línea tienen efectos directos en el mundo real, pues pretende propagar posturas atentatorias a los derechos humanos que lamentablemente son puestas en práctica por personas o grupos que se alimentan de la intolerancia. De esta manera, Internet debe ser usado positivamente, como mecanismo para propagar ideas de libertad, democracia y respeto de los derechos humanos y constituirse en un espacio sano, seguro y constructivo en el que niños, niñas, adolescentes, mujeres y, en general cualquier persona, pueda desarrollarse, libre de cualquier tipo violencia.

2.4.9 Resolución 71/199, sobre el derecho a la privacidad en la era digital, de 19 de diciembre de 2016.

La Asamblea General de las Naciones Unidas aprueba la Resolución 71/199, sobre el derecho a la privacidad en la era digital, de 19 de diciembre de 2016[1108], en la cual se reconocen las situaciones que se han desarrollado en los últimos años y que ameritan nuevas posturas respecto de los derechos de las personas:

> […] f) Elaboren o mantengan y apliquen una legislación adecuada, con sanciones y recursos eficaces que protejan a las personas contra las violaciones y las transgresiones del derecho a la privacidad, concretamente la recopilación y el tratamiento ilegales y arbitrarios, la retención o el uso de datos personales por particulares, gobiernos, empresas y organizaciones privadas;

[1107] Ibíd.
[1108] ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, "Resolución 71/199, sobre el derecho a la privacidad en la era digital, 2016, accedido el 12 de agosto de 2019, https://undocs.org/pdf?symbol=es/A/RES/71/199

> g) Sigan elaborando o manteniendo, a ese respecto, medidas preventivas y procedimientos de recurso para las violaciones y transgresiones del derecho a la privacidad en la era digital, que pueden afectar a todas las personas, incluidas, con repercusiones particulares, las mujeres, así como los niños y quienes son vulnerables o están marginados;
> h) Promuevan una educación de calidad y oportunidades de educación permanente para todos, a fin de fomentar, entre otras cosas, los conocimientos digitales y las aptitudes técnicas necesarias para proteger eficazmente la privacidad;
> i) Se abstengan de exigir a las empresas que adopten medidas que interfieran con el derecho a la privacidad de manera arbitraria o ilegal;
> j) Consideren medidas apropiadas para que las empresas puedan adoptar las medidas voluntarias de transparencia adecuadas en relación con las solicitudes de las autoridades estatales que requieren acceso a datos e información privada de los usuarios;
> k) Elaboren o mantengan legislación, medidas preventivas y compensatorias ante los daños derivados de la venta, la reventa múltiple u otros intercambios mercantiles de datos personales sin el consentimiento libre, explícito y fundado de los interesados; […][1109]

De lo citado se colige que, la necesidad de intervención estatal que garantice la protección de las personas y sus datos se torna indispensable. Ya no solo se trata de elaborar normas adecuadas sino que estas sean efectivas a través de acciones, procedimientos de reclamo y sanciones no solo a empresas y organismos privados sino al propio Estado, de ser el caso.

Pero además, se visibiliza la necesidad de establecer un régimen preventivo para proteger a mujeres y niños principalmente, con énfasis en su educación.

Finalmente, la reparación además de permitir reparar económicamente y recomponer en otras esferas, a la víctima por el daño causado. El valor económico y logístico de la indemnización se vuelva, para el infractor, un mecanismo disuasivo que evite el tratamiento y comunicación de datos personales sin el consentimiento del titular.

Debido a la naturaleza de las transgresiones que pueden sufrir las personas, por la masiva acumulación de datos personales y los consecuentes riesgos a los que se expone a sus titulares, la citada resolución exhorta no solo a los Estados miembros de las Naciones Unidas sino también a las empresas a cumplir las siguientes recomendaciones:

> […] a) Cumplan su responsabilidad de respetar los derechos humanos, de conformidad con los Principios Rectores sobre las Empresas y los Derechos Humanos: Puesta en Práctica del Marco de las Naciones Unidas para "Proteger, Respetar y Remediar"12, incluido el derecho a la privacidad en la era digital;
> b) Informen a los usuarios sobre la recopilación, el uso, el intercambio y la retención de los datos que puedan afectar su derecho a la privacidad y establezcan políticas de transparencia, cuando corresponda;
> 7. Alienta a las empresas a que trabajen para facilitar las comunicaciones seguras y la protección de los usuarios individuales contra injerencias arbitrarias o ilegales en su privacidad, incluso mediante el desarrollo de soluciones técnicas; […][1110]

De lo dicho, se insta a las empresas a establecer mecanismos de protección de la privacidad, incluyendo comunicaciones seguras evitando injerencias a la privacidad de

[1109] Ibíd.
[1110] Ibíd.

los usuarios, pero sobretodo, se determina la responsabilidad de los privados de garantizar el respeto de los derechos humanos, para lo cual es necesario que las relaciones de lealtad y transparencia entre usuario y empresa sean respetadas y potenciadas.

2.4.10 Resolución 34/7 sobre el derecho a la privacidad en la era digital, el 23 de marzo de 2017

La Resolución 34/7, sobre el derecho a la privacidad en la era digital aprobada por el Consejo de Derechos Humanos, el 23 de marzo de 2017[1111] recoge lo dispuesto en las anteriores resoluciones 28/16 y 71/199 sobre como este derecho se ha convertido en un baluarte para la democracia y el ejercicio de otros derechos humanos en Internet. En esta versión se recoge ahora nuevas formas de transgresión y además se hacen consideraciones adicionales de como los Estados y los particulares pueden hacer frente a las violaciones producidas en el entorno digital.

> [⋯] 5. Alienta a todos los Estados a que promuevan un entorno de tecnología de la información y las comunicaciones abiertas, seguras, estables, accesibles y pacíficas, basadas en el respeto del derecho internacional, incluidas las obligaciones consagradas en la Carta de las Naciones Unidas y los instrumentos de derechos humanos; 7. Alienta a todas las partes interesadas pertinentes
>
> 8. Exhorta a todas las empresas a que asuman su responsabilidad de respetar los derechos humanos de conformidad con los Principios Rectores sobre las Empresas y los Derechos Humanos: Puesta en Práctica del Marco de las Naciones Unidas para "Proteger, Respetar y Remediar", incluido el derecho a la privacidad en la era digital, e informen a los usuarios sobre la recopilación, el uso, la distribución y la retención de sus datos que puedan afectar a su derecho a la privacidad y establezcan una transparencia y unas políticas que permitan el consentimiento informado de los usuarios, según proceda;
> 9. Alienta a las empresas a que busquen soluciones técnicas que aseguren y protejan la confidencialidad de las comunicaciones digitales, que pueden comprender medidas de cifrado y anonimato, y exhorta a los Estados a que no interfieran en el uso de esas soluciones técnicas y que toda restricción al respecto esté en conformidad con las obligaciones de los Estados en virtud del derecho internacional de los derechos humanos; [⋯] [1112]

Se reconoce a Internet como un espacio en el que los distintos tratados y convenios sobre derechos humanos deben cumplirse. Pero además, establece que los Principios Rectores sobre las Empresas y los Derechos Humanos[1113] dictado en el año 2011, por los cuales no solo el Estado sino los particulares están en la obligación de "Proteger, Respetar y Remediar" los derechos de las personas, incluyen entre estos, el derecho a la

[1111] ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Resolución 34/7 sobre el derecho a la privacidad en la era digital*, 2017, accedido el 12 de agosto de 2019, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/36/PDF/G1708636.pdf?OpenElement
[1112] Ibíd.
[1113] CONSEJO DE DERECHOS HUMANOS, *Resolución 17/4 sobre Principios Rectores sobre las empresas y los derechos humanos*, 2011, accedido el 12 de agosto de 2019, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf

privacidad. Estos principios fundacionales y operativos atienden a la responsabilidad de las empresas de respetar los derechos humanos, de tal manera que se eviten

> [⋯] que sus propias actividades provoquen o contribuyan a provocar consecuencias negativas sobre los derechos humanos y hagan frente a esas consecuencias cuando se produzcan; b) Traten de prevenir o mitigar las consecuencias negativas sobre los derechos humanos directamente relacionadas con operaciones, productos o servicios prestados por sus relaciones comerciales, incluso cuando no hayan contribuido a generarlos[1114].

En suma, las empresas son también responsables de transgresiones en la era digital y por ello están obligadas a prevenir en sus modelos de negocios y productos, así como responsabilizarse por los daños que pudieran haber causado.

2.4.11 Resolución 38/7 sobre promoción, protección y disfrute de los derechos humanos en Internet, el 5 de julio de 2018.

La Resolución 38/7 sobre promoción, protección y disfrute de los derechos humanos en Internet, aprobada por el Consejo de Derechos Humanos de 5 de julio de 2018[1115] identifica a la seguridad como factor fundamental para evitar la violencia digital, por ello:

> […] 8. Exhorta a los Estados a hacer frente a los problemas de seguridad en Internet de conformidad con sus obligaciones internacionales de derechos humanos para garantizar la protección en línea de todos los derechos humanos, en particular la libertad de opinión y de expresión, la libertad de asociación y la privacidad, especialmente por conducto de instituciones nacionales democráticas y transparentes, sobre la base del estado de derecho, y de un modo que garantice la libertad y la seguridad en Internet para que esta pueda seguir siendo una fuerza dinámica que genere desarrollo económico, social y cultural; […][1116]

Asimismo, establece la importancia de que las empresas busquen medidas técnicas para garantizar la confidencialidad de las comunicaciones, el anonimato y el cifrado, como mecanismos necesarios para propiciar una internet más libre que respete la libertad de expresión y la privacidad, al tenor de lo siguiente:

> […]9. Alienta a las empresas comerciales a que traten de encontrar soluciones técnicas propicias para asegurar y proteger la confidencialidad de las comunicaciones digitales, que puedan incluir medidas de codificación y anonimato, y exhorta a los Estados a no interferir en el uso de esas soluciones técnicas, y que cualquier restricción a las mismas se ajuste a las obligaciones que tienen los Estados en virtud del derecho internacional de los derechos humanos; […][1117]

[1114] CONSEJO DE DERECHOS HUMANOS DE LAS NACIONES UNIDAS, *Resolución 17/4 sobre Principios Rectores sobre las empresas y los derechos humanos*, 2011, accedido el 12 de agosto de 2019, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf

[1115] ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Resolución 38/7 sobre el derecho a la privacidad en la era digital*, 2018, accedido el 12 de agosto de 2019, http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/RES/38/7&Lang=S

[1116] Ibíd.

[1117] Ibíd.

Establece la obligación de que los Estados asuman su obligación de formar y generar conciencia en la población respecto de la existencia de noticias falsas que pueden estar manipulando sus decisiones, especialmente aquellas relacionadas con la decisión sobre el voto democrático y la participación en el foro público.

> […]16. Exhorta a los Estados a que, respetando plenamente sus obligaciones y compromisos de derechos humanos en relación con la libertad de opinión y de expresión, fomenten a la vez la capacitación de los medios de comunicación, campañas educativas y demás actividades destinadas a detectar la información en línea que pueda ser deliberadamente engañosa o falsa y a crear conciencia sobre esa información; 17. Insta a los Estados a adoptar, aplicar y, de ser necesario, reformar leyes, reglamentos, políticas y medidas relativas a la protección en línea de los datos personales y la privacidad para prevenir, mitigar y remediar la recolección, la retención, el procesamiento, el uso o la revelación arbitrarios o ilícitos de datos personales en Internet que pudieran violar los derechos humanos; […][1118]

Determina que para la promoción, protección y disfrute de los derechos humanos en Internet es indispensable apuntalar el acceso universal, porque solo a través de la libertad se puede construir sociedades más equitativas.

> […]18. Exhorta a los Estados a considerar la posibilidad de formular, mediante procesos transparentes e inclusivos con todas las partes interesadas, y de adoptar políticas públicas nacionales relativas a Internet que tengan como objetivo principal el acceso universal y el disfrute de los derechos humanos; […][1119]

Podemos observar que paulatinamente se va definiendo la necesidad de que todo el ecosistema digital coadyuve simultáneamente la generación de espacios digitales accesibles, libres de violencia y resilientes. Sin duda, la tecnología es un elemento fundamental para el desarrollo de los pueblos y por ende debe garantizarse que su uso fomente el ejercicio de derechos humanos.

2.4.12 Resolución 73/199, sobre el derecho a la privacidad en la era digital, de 17 de diciembre de 2018.

La Asamblea General, el 17 de diciembre de 2018, aprueba la Resolución 73/199 sobre el derecho a la privacidad en la era digital[1120], en la que se hace un análisis de las nuevas problemáticas que plantean retos para la protección de las personas y sus datos personales.

El capítulo III del Informe A/HRC/39/29 sobre el derecho a la privacidad en la era digital, que sustenta la citada resolución[1121] determina los casos de injerencias a la privacidad, entre los que destaca, el uso creciente de datos personales por Gobiernos y empresas:

[1118] Ibíd.
[1119] Ibíd.
[1120] ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Resolución 73/199, sobre el derecho a la privacidad en la era digital*, 2018, accedido el 12 de agosto de 2019, https://undocs.org/pdf?symbol=es/A/RES/73/179
[1121] ALTO COMISIONADO DE LAS NACIONES UNIDAS PARA LOS DERECHOS HUMANOS, *Informe A/HRC/39/29 sobre el derecho a la privacidad en la era digital*, 2018, accedido el 13 de octubre de 2019, https://undocs.org/A/HRC/39/29

a) *Aumento de la huella digital:* Los Estados y las empresas reúnen y utilizan una cantidad cada vez mayor de datos relacionados con la vida privada de las personas. La información que se reúne y utiliza es enorme y abarca desde identificadores de dispositivos, direcciones de correo electrónico y números de teléfono hasta datos biométricos, médicos, financieros y pautas de conducta. Muchas de esas actividades se realizan sin el conocimiento de las personas afectadas y sin su consentimiento válido. [1122]
b) *Intercambio y fusión de datos:* Las empresas y los Estados intercambian y fusionan constantemente datos personales procedentes de diversas fuentes y bases de datos. Como resultado, las personas se encuentran en una posición de indefensión, por la dificultad que entraña llevar un seguimiento de quién tiene información sobre ellas y de qué tipo de información se trata, y aún más controlar las múltiples formas en que puede ser utilizada.
c) *Datos biométricos:* Estos son datos particularmente delicados y pueden ser objeto de vulneraciones graves. Al recopilar datos biométricos se debe prestar atención a los principios de necesidad y proporcionalidad.
d) *Aumento de la capacidad de análisis:* Muchos de los sistemas utilizados por los gobiernos y las empresas han sido creados con ese fin preciso: obtener la mayor cantidad posible de información sobre las personas a fin de analizarlas, establecer sus perfiles, evaluarlas, clasificarlas y, en última instancia, adoptar decisiones, a menudo automatizadas, acerca de ellas.

Respecto de la vigilancia e interceptación de las comunicaciones por los Estados[1123] el informe de la relatoría especial señala lo siguiente:

a) *Vigilancia a gran escala:* Algunos Estados afirman que esa vigilancia en masa e indiscriminada es necesaria para proteger la seguridad nacional, esta práctica no es permisible en virtud del derecho internacional de los derechos humanos. El Tribunal Europeo de Derechos Humanos ha señalado que un sistema de vigilancia secreta creado para proteger la seguridad nacional puede socavar o incluso destruir la democracia con el pretexto de defenderla.
b) *Acceso a los datos de los usuarios de las empresas:* Los Estados suelen recurrir a las empresas para recopilar e interceptar datos personales. Esos sistemas de acceso directo suscitan una gran preocupación, ya que son particularmente propicios a los abusos y tienden a eludir las garantías procesales fundamentales.
c) *Piratería informática:* Esto comporta riesgos que no solo afectan al derecho a la intimidad, sino también a los derechos a la equidad procesal respecto del uso de estas pruebas en las actuaciones judiciales.
d) *Intentos de debilitar el cifrado y el anonimato:* Las herramientas de cifrado y anonimato son muy utilizadas en todo el mundo, en particular por los defensores de los derechos humanos, la sociedad civil, los periodistas, los denunciantes de irregularidades y los disidentes políticos que son objeto de persecución y acoso.

[1122] *Ibíd.*
[1123] *Ibíd.*

e) *Intercambio de información de inteligencia:* Los Gobiernos de todo el mundo suelen intercambiar información sobre personas sin sujeción a un marco jurídico ni a una supervisión adecuada.
f) *Acceso transfronterizo a los datos de las empresas:* Resulta particularmente preocupante que los Estados en los que el estado de derecho es deficiente o tienen un historial problemático de derechos humanos puedan obtener acceso a información personal sensible sin protección adecuada frente a las posibles vulneraciones de los derechos humanos.

En cuanto al capítulo IV titulado "Responsabilidades de los Estados", del informe A/HRC/39/29 sobre el derecho a la privacidad en la era digital[1124] se señala lo siguiente:

a) *Responsabilidad de los Estados de respetar y obligación de proteger el derecho a la privacidad en la era digital:* El deber de los Estados de proteger contra las vulneraciones del derecho a la vida privada por parte de las empresas y otros terceros constituidos o domiciliados en su jurisdicción tiene efectos extraterritoriales.[1125]
b) Responsabilidad del Estado de establecer salvaguardias adecuadas y una supervisión eficaz, en cuanto al marco general de protección contra injerencias indebidas: El marco de protección de la privacidad de un Estado debe basarse en leyes que establezcan las normas para el tratamiento de la información personal, tanto por los Estados como por agentes privados. Las personas cuyos datos personales se están tratando deberían ser informadas sobre el tratamiento de datos, sus circunstancias, su carácter y su alcance, entre otras cosas mediante políticas transparentes de protección de datos. Las personas afectadas tienen derecho a saber que sus datos personales se han conservado y tratado, a acceder a los datos almacenados, a rectificar los datos inexactos u obsoletos y a suprimir o corregir los datos almacenados de manera ilícita o innecesaria. Es importante que el marco jurídico garantice que esos derechos no limiten el derecho a la libertad de expresión, incluido el tratamiento de datos personales para fines periodísticos, artísticos y académicos. Los marcos para la protección de datos también deben imponer ciertas obligaciones a las entidades que tratan datos personales. Las transferencias de datos, en particular de grandes cantidades de datos personales, son una práctica común que resulta necesaria para el funcionamiento de muchos servicios. Los Estados deben velar por que esas transferencias no conlleven o faciliten la injerencia indebida en el derecho a la privacidad. Los Estados deben establecer órganos de supervisión independientes para el tratamiento de datos personales. La autoridad de supervisión debe contar con una base jurídica que establezca claramente su mandato, sus atribuciones y su independencia.

[1124] ALTO COMISIONADO DE LAS NACIONES UNIDAS PARA LOS DERECHOS HUMANOS, *Informe A/HRC/39/29 sobre el derecho a la privacidad en la era digital*, 2018, accedido el 13 de octubre de 2019, https://undocs.org/A/HRC/39/29
[1125] PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS, artículo 2, párrafo 1, parte II, 23 de marzo de 1976, https://bit.ly/2tJBadx

c) *Salvaguardias de procedimiento y supervisión de la vigilancia y la interceptación de las comunicaciones:*
    1. *Salvaguardias:* En virtud de los principios de necesidad y proporcionalidad, hay excepciones que deberían limitarse a fin de garantizar un nivel adecuado de protección de los datos en todos los poderes del Estado.
    2. *Autorización y supervisión independientes:* El órgano independiente que autoriza las medidas de vigilancia concretas, preferiblemente una autoridad judicial, debe asegurarse de que existen pruebas claras de una amenaza lo suficientemente importante y que la propuesta de vigilancia tiene un fin específico y es estrictamente necesaria y proporcional, para autorizar o no las medidas de vigilancia. Los órganos de supervisión deben ser independientes de las autoridades que llevan a cabo la vigilancia, disponer de conocimientos técnicos, competencias y recursos. La autorización y la supervisión deben estar a cargo de distintas instituciones.
    3. *Principio de transparencia:* Las autoridades estatales y los órganos de supervisión también deberían informar al público de las leyes, políticas y prácticas vigentes en materia de vigilancia e interceptación de las comunicaciones y otras formas de tratamiento de los datos personales, ya que el debate y el escrutinio público son esenciales para comprender las ventajas y limitaciones de las técnicas de vigilancia.

Respecto del capítulo V sobre responsabilidades de las empresas el informe de la relatoría especial señala que: Las empresas que recopilan y conservan datos de sus usuarios deben evaluar los riesgos para la privacidad asociados a las potenciales peticiones de esos datos por parte de los Estados, en particular el entorno jurídico e institucional de los Estados en cuestión.

En cuanto al capítulo VI sobre mecanismos de reparación el informe de la relatoría especial señala que: Entre los mecanismos estatales extrajudiciales competentes en la esfera de las TIC están las autoridades independientes con facultades para supervisar las prácticas del Estado y el sector privado en la esfera de la protección de datos, como los organismos de protección de la privacidad y los organismos de protección de datos. Las empresas deberían informar a sus clientes cuando tomasen conocimiento de la existencia de filtraciones de datos personales que podrían haber afectado a sus derechos.

En cuanto al capítulo VII. Conclusiones y recomendaciones el informe de la relatoría especial señala que: El marco internacional de derechos humanos ofrece una base sólida para formular respuestas a los múltiples desafíos que se plantean en la era digital. Los Estados deben establecer un marco jurídico y normativo apropiado, en particular leyes y reglamentos adecuados sobre protección de la privacidad que incorporen los principios de legalidad, proporcionalidad y necesidad, y establezcan salvaguardias y mecanismos de supervisión y reparación.

Volviendo a la resolución Resolución 73/199 sobre el derecho a la privacidad en la era digital[1126] se establece la necesidad de nombrar autoridades nacionales independientes que realmente cumplan roles de prevención, regulación, orientación, pero sobre todo de vigilancia y sanción que permita un efectivo cumplimiento de la protección de los datos y de las comunicaciones digitales, al tenor de lo siguiente:

> [⋯] g) Examinen la posibilidad de adoptar y aplicar leyes, normas y políticas de protección de datos, incluidos los datos de las comunicaciones digitales, que se ajusten a sus obligaciones internacionales en materia de derechos humanos, que podrían incluir el establecimiento de autoridades nacionales independientes con las facultades y los recursos necesarios para supervisar las prácticas de protección de datos, investigar las violaciones y los abusos y recibir comunicaciones de particulares y organizaciones, y ofrecer vías de recurso adecuadas; [⋯][1127]

El traslado de la violencia de género de los espacios físicos a los digitales establece la necesidad de propiciar la igualdad y la erradicación de estereotipos intolerantes.

> [⋯] i) Consideren la posibilidad de elaborar, examinar, aplicar y fortalecer políticas con perspectiva de género que promuevan y protejan el derecho de todas las personas a la privacidad en la era digital; [⋯][1128]

En cuanto a las empresas la resolución recomienda el desarrollo e implementación de medidas técnicas que garanticen un uso respetuoso de los datos en el contexto del respeto de los derechos humanos de sus titulares. Llama la atención, la definición de principios como el de finalidad, el de calidad, el de confidencialidad, el de licitud, la limitación de las decisiones automatizadas, la responsabilidad demostrada que determina una actuación diligente de los responsables del tratamiento. En suma, en los textos que se citan a continuación se reconoce varios de los principios que aparecen contemplados en el RGPD y en varias de las legislaciones latinoamericanas inspiradas en el modelo europeo, ya que ofrecen el estándar más alto de protección garantista de derechos:

> [⋯] c) Apliquen salvaguardas administrativas, técnicas y físicas para garantizar que los datos se procesen de manera lícita y que este procesamiento se limite a lo necesario en relación con sus fines, y que se aseguren la legitimidad de estos fines y la precisión, integridad y confidencialidad del procesamiento;
> d) Velen por que se incorporen el respeto del derecho a la privacidad y otros derechos humanos reconocidos internacionalmente en el diseño, funcionamiento, evaluación y regulación de la adopción automatizada de decisiones y las tecnologías de aprendizaje automático y prevean recursos para remediar los abusos de los derechos humanos que hayan causado o a los que hayan contribuido; [⋯]
> j) Proporcionen una orientación eficaz a las empresas sobre la forma de respetar los derechos humanos mediante el suministro de asesoramiento sobre métodos apropiados,

[1126] ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Resolución 73/199, sobre el derecho a la privacidad en la era digital*, 2018, accedido el 12 de agosto de 2019, https://undocs.org/pdf?symbol=es/A/RES/73/179
[1127] ASAMBLEA GENERAL DE LAS NACIONES UNIDAS, *Resolución 73/199, sobre el derecho a la privacidad en la era digital*, 2018, accedido el 12 de agosto de 2019, https://undocs.org/pdf?symbol=es/A/RES/73/179
[1128] *Ibíd.*

> incluida la diligencia debida en materia de derechos humanos, y sobre la manera de considerar eficazmente las cuestiones de género, vulnerabilidad o marginación;[⋯] [1129]

Finalmente, la resolución recomienda que el Consejo de Derechos Humanos y a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, así como todas las partes interesadas:

> [⋯] sigan examinando la forma en que la elaboración de perfiles, la adopción automatizada de decisiones y las tecnologías de aprendizaje automático, a veces denominadas inteligencia artificial, cuando no cuentan con las salvaguardas debidas repercuten en el disfrute del derecho a la privacidad, con el fin de aclarar los principios y las normas existentes y determinar las mejores prácticas de promoción y protección de ese derecho [⋯] [1130]

Es decir, que sobre nuevas tecnologías como la inteligencia artificial se insta a que se establezcan principios, obligaciones y salvaguardas que impidan posibles transgresiones. Puesto que, es tan complejo anticipar las posibles consecuencias de los avances tecnológicos que es ineludible realizar el mayor esfuerzo posible por buscar un equilibrio entre el desarrollo técnico-científico, la ética y el respeto de los derechos humanos.

2.5 Estándares de Protección de Datos Personales para Estados Iberoamericanos

Si bien existen iniciativas en la región, como las llevadas a cabo por los distintos organismos internacionales de la región: Organización de Estados Americanos, Corte Interamericana de Derechos Humanos, o incluso la Organización de Naciones Unidas. Dichas resoluciones o recomendaciones, no han tenido la suficiente fuerza para conseguir una armonización ni homogenización del sistema de protección de datos en Latinoamérica. Uno de los motivos, sin descartar otros que pudieran tener mucho más peso como las realidades sociopolítica y económica de Latinoamérica, puede ser la falta de precisión y conocimiento técnico específico sobre esta temática tan compleja. Por este motivo, la Agencia Española de Protección de Datos, desde el año 2003 junto con varios países latinoamericanos asistentes al II Encuentro Iberoamericano de Protección de Datos, constituyó la Red Iberoamericana de Protección de datos como órgano encargado "de buscar y sugerir en su caso soluciones armonizadas, y apoyar iniciativas de sus miembros de difundir y desarrollar la cultura de protección de datos personales en los países Iberoamericanos en un contexto democrático". [1131]

Como parte de los objetivos cumplidos, la señalada Red, en el XV Encuentro Iberoamericano de Protección de Datos, aprobó los "Estándares de Protección de Datos de los Estados Iberoamericanos", el 20 de junio de 2017. Este texto constituye una propuesta que pretende impulsar la cooperación efectiva relacionada con la protección de datos personales y privacidad en Latinoamérica, pero además fortalecer los procesos regulatorios de la región, así como promover la actualización de aquellas normativas existentes. En suma, propone estándares flexibles que permitan la adopción de su contenido, sin contravenir de ninguna manera su derecho interno.

[1129] *Ibíd.*
[1130] *Ibíd.*
[1131] II ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS, *Declaración de la Antigua (Guatemala)*, 6 de junio del 2003, accedido el 2 de noviembre de 2019, http://www.redipd.es/documentacion/common/declaracion_2003_II_encuentro_es.pdf

Entre los objetivos de los Estándares Iberoamericanos destacan varios:

- Establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región.
- Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales.
- Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región.
- Favorecer la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y autoridades y organismos internacionales en la materia.
- Garantiza un nivel adecuado de protección de los datos personales en la región iberoamericana, con la finalidad de no establecer barreras a la libre circulación de éstos en los Estados Iberoamericanos y, en consecuencia, favorecer las actividades comerciales entre la región, así como con otras regiones económicas.[1132]

A continuación se identificará el contenido esencial del derecho a la protección de datos en esta propuesta.

a) Ámbito: Registros o ficheros públicos y privados

El estándar propone tres ámbitos de aplicación: el primero denominado subjetivo, el segundo, objetivo, y el tercero, el territorial que constan en los preceptos 3, 4 y 5 de los estándares.

Acerca del *ámbito de aplicación subjetivo*, los estándares proponen que la normativa sea aplicable a personas físicas o jurídicas de carácter privado, autoridades y organismos públicos, que traten datos personales en el ejercicio de sus actividades y funciones. Es decir, esta norma regula a quienes tratan datos personales en cualquier ámbito público o privado. Se clarifica la postura latinoamericana que ha regulado solo en el ámbito público este derecho como es el caso del El Salvador y Guatemala, o que ha tenido que dictar dos normas que incluso desfasan en tiempo como es el caso de México, cuya norma de protección de datos particulares data de 2010, mientras que la aplicable a las entidades públicas es del año 2017.

Respecto del *ámbito de aplicación objetivo*, recomienda que las normas de protección de datos deban ser aplicables al tratamiento de datos personales que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización. Con lo cual, se zanjan varias dudas respecto de la naturaleza de la base de datos. Además, se reconoce lo avanzada de la norma pues incluye todo tipo de tratamientos y soportes en aras de proteger los datos personales.

[1132] RED IBEROAMERICANA DE PROTECCIÓN DE DATOS PERSONALES, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*, de 20 de junio de 2017, accedido el 2 de noviembre de 2019,http://www.redipd.org/noticias_todas/2017/novedades/common/Estandares_Esp_Con_logo_RIPD.pdf#Testo%20en%20espa%C3%B1ol.

Los estándares señalan que la normativa debe proteger los datos personales de personas físicas, aunque deja a criterio de cada Estado la protección de las personas jurídicas. Esta aclaración se produce al margen de la postura europea, precisamente porque es Latinoamérica donde el garantismo constitucional ha tenido mayor acogida y por ello varias Constituciones, como la ecuatoriana y la colombiana, reconocen derechos fundamentales a las personas jurídicas siempre en atención a las condiciones específicas de cada situación que se reclame.

Además, el estándar sugiere que no se aplique el contenido de esta normativa a los datos personales familiares o domésticos de una persona física, es decir, datos personales en un entorno de amistad, parentesco o grupo personal cercano y que no tengan como propósito una divulgación o utilización comercial. Esta claridad de la norma sugerida libera de la discusión del alcance del término doméstico; además limita a que solo las personas físicas pueden ser sujetos de esta excepción específica.

Si bien varias legislaciones latinoamericanas no contemplan dentro de su glosario de término las características de la información anónima, el estándar propone que se la conceptualice como aquella que no guarda relación con una persona física identificada o identificable, así como los datos personales sometidos a un proceso de anonimización, de tal forma que el titular no pueda ser identificado o reidentificado. Dicho de otro modo, aclara que el dato puede ser anónimo *per se* o puede, mediante un tratamiento de anonimización, llegar a serlo. En el mismo sentido, la norma 2 relativa a las definiciones señala que este proceso se produce por medio de la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados.

Respecto del tercer *ámbito de aplicación denominado territorial*, los estándares serán aplicables al tratamiento de datos personales cuando estos se hayan efectuado por un responsable o encargado establecido en territorio de los Estados iberoamericanos. En el caso de que no se encuentre establecido en territorio de los Estados iberoamericanos, sus actividades de tratamiento estarán relacionadas con la oferta de bienes o servicios dirigidos a los residentes de estos Estados, o bien, estén relacionadas con el control de su comportamiento, en la medida en que este tenga lugar en los Estados iberoamericanos. Otro caso es por un responsable o encargado que no esté establecido en un Estado iberoamericano, pero le resulte aplicable la legislación nacional de dicho Estado, derivado de la celebración de un contrato o en virtud del derecho internacional público. Finalmente, por un responsable o encargado no establecido en territorio de los Estados iberoamericanos y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito. Es decir, se propone un modelo de cobertura similar al europeo, como estrategia de universalizar esta forma de protección y de aplicación extraterritorial.

Se destaca la claridad del estándar al definir que debe entenderse por establecimiento, señalando que es el lugar de la administración central o principal del responsable o encargado, el cual deberá determinarse en función de criterios objetivos e implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones respecto a los fines y medios del tratamiento de datos personales que lleve a cabo, mediante modalidades estables. No siendo suficiente la sola presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o

las actividades de tratamiento. Se agrega que si el tratamiento de datos personales lo realiza un grupo empresarial, el establecimiento principal de la empresa que ejerce el control deberá considerarse establecimiento principal, excepto cuando los fines y medios del tratamiento los determine efectivamente otra de las empresas del grupo.

b) Naturaleza del dato

Respecto de la naturaleza del dato, los estándares en el precepto 2, relativo a las definiciones, proponen que se entenderá por datos personales cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas. Este concepto recoge los principales avances en la determinación de la naturaleza del dato, pues incluye la condición de que una persona identificable lo es únicamente si los plazos o actividades para conocer su identidad no son desproporcionados.

De otro lado, la misma norma señala que los datos personales sensibles son aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para este. Se destaca que la enumeración que realiza de varios datos considerados sensibles es meramente enunciativa a diferencia de algunas de las legislaciones latinoamericanas que las señala de forma taxativa. Estos son aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, y de los cuales los datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física son aquellos que no estaban incorporados en las versiones legales y que ahora aparecen en esta enumeración. Todo lo cual da cuenta de la necesidad de que la lista sea *numerus apertus* debido a los cambios vertiginosos que se producen en estos temas por los continuos avances tecnológicos.

Finalmente, la citada norma señala la definición de tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales relacionados, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

c) Sujeto activo

Conforme el precepto 2 de los estándares relativos a las definiciones, se considera como titular a la persona física a quien le conciernen los datos personales. No obstante, como se mencionó en líneas anteriores, se deja a cada Estado la posibilidad de regular la protección de los datos de personas jurídicas, de tal manera que de esta forma se le puede otorgar una titularidad acotada a ciertos casos o ámbitos específicos de protección asociadas al reconocimiento que en varias normativas tienen las personas jurídicas como titulares de determinados derechos fundamentales.

En el precepto número 32.3 de los estándares se propone que las personas físicas vinculadas a fallecidos o designados por estos, puedan ejercer los derechos a que se refiere el presente estándar respecto a los datos personales de fallecidos que les conciernan; esto es los derechos ARCO.

d) Sujeto pasivo

El citado precepto 2 sobre definiciones determina que son sujetos pasivos y por ende obligados por la presente normativa: el responsable, el encargado y el exportador.

El responsable es la persona física o jurídica de carácter privado, autoridad pública, servicio u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

El exportador es la persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales.

El encargado es el prestador de servicios que, con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de este.

Conforme señala el precepto 33 de los Estándares, se determina que el encargado realizará las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitará sus actuaciones a los términos fijados por el responsable, para lo cual necesita la formalización de la prestación de servicios del encargado mediante la suscripción de un contrato o cualquier otro instrumento jurídico aplicable en la materia que contendrá, al menos, el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento; el tipo de datos personales; las categorías de titulares, así como las obligaciones y responsabilidades del responsable y encargado. Así como, la expresa mención de que realiza el tratamiento de los datos personales conforme a las instrucciones del responsable. De no contar con esta instrumentación, debe abstenerse de tratar los datos personales y tampoco hacerlo para finalidades distintas a las instruidas por el responsable. Está obligado, además, a implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables, informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones, guardar confidencialidad respecto de los datos personales tratados, suprimir, devolver o comunicar a un nuevo encargado designado por el responsable los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones de este, excepto que una disposición legal exija la conservación de los datos personales, o bien que el responsable autorice la comunicación de estos a otro encargado, abstenerse de transferir los datos personales, salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad de control; permitir al responsable o autoridad de control inspecciones y verificaciones en sitio; asumir la calidad de responsable si incumple sus obligaciones.

El encargado a su vez podrá subcontratar servicios que impliquen el tratamiento de datos personales, siempre y cuando exista una autorización previa por escrito, específica o general del responsable, o bien se estipule expresamente en el contrato o instrumento

jurídico suscrito entre este último y el encargado. De esta manera, el subcontratado asumirá el carácter de encargado y de no cumplir con sus obligaciones, asumirá la calidad de responsable.

Estas precisiones respecto del encargado son producto de las confusiones y erróneas aplicaciones que se han producido en el quehacer cotidiano de los procesos, lo cual ha motivado la necesidad de esta normativa específica.

e) Objeto o bien jurídico

a. Derecho de información:

No consta en los estándares el derecho de información.

b. Autodeterminación informativa

En el inciso 2 de la exposición de motivos del estándar iberoamericano se aclara que el derecho a la protección de datos personales se ha:

> [...] conceptualizado en algunos países Iberoamericanos, legislativamente o jurisprudencialmente, como un derecho de naturaleza distinta a los derechos a la vida privada y familiar, a la intimidad, al honor, al buen nombre y otros derechos similares, que en su conjunto garantizan el libre desarrollo de la personalidad de la persona física, hasta conformarse en un derecho autónomo, con características y dinámica propias, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona física con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.[1133]

Es decir, al constar en este documento el derecho a decidir sobre la entrega, tratamiento y cesión de sus datos personales, se está reconociendo expresamente el derecho a la autodeterminación informativa como elemento esencial del derecho a la protección de datos personales y contenido esencial que lo distingue de otros y marca su autonomía e independencia.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

Conforme el precepto 6 de los Estándares, se sugiere a los Estados limitar el derecho a la protección de datos, de forma adecuada y proporcional en una sociedad democrática, debiendo respetar los derechos y las libertades fundamentales de los titulares. Dicha limitación debe constar de forma expresa en la ley, en los siguientes casos: salvaguardar la seguridad nacional, la seguridad pública, la protección de la salud pública, la protección de los derechos y las libertades de terceros, así como por cuestiones de interés público.

Además, deberá mencionarse específicamente que las limitaciones se refieren a la finalidad del tratamiento, las categorías de datos personales, el alcance de las limitaciones, las garantías adecuadas para evitar accesos o transferencias ilícitas o

[1133] RED IBEROAMERICANA DE PROTECCIÓN DE DATOS PERSONALES, 20/06/2017.

desproporcionadas, la determinación del responsable o responsables, los plazos de conservación de los datos personales, los posibles riesgos para los derechos y libertades de los titulares, el derecho de los titulares a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a los fines de esta.

d. Principios

i. Deber de información o transparencia

No consta en los estándares este principio con esta denominación, sino con la de "transparencia", ya que se establece la obligación de que todo responsable cuente con políticas transparentes de los tratamientos de datos personales que realice.

El estándar 16 recoge el principio de transparencia por el cual el responsable informará al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. Entre la información que el responsable tiene la obligación de proporcionar consta, al menos, la siguiente: a) La identidad y datos de contacto del responsable; b) Las finalidades del tratamiento a que serán sometidos sus datos personales; c) Las comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y las finalidades que motivan la realización de las mismas; d) La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad; e) El origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular.

Además, la información proporcionada al titular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los titulares a quienes va dirigida, especialmente si se trata de niñas, niños y adolescentes.

ii. Pertinencia o proporcionalidad

No consta en los estándares este principio con esta denominación, debido a que solía confundirse con el de calidad. En tal caso, en el estándar se denomina "proporcionalidad", el cual señala que el responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento, tal como señala el precepto 18 del estándar.

iii. Calidad

El estándar numero 19 señala que el responsable adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de estos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento. Se anota que cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable los eliminará. Es importante destacar el detalle de la norma, pues para dejar fuera toda duda se aclara que la eliminación se hará no solo de los archivos, registros o bases de datos, sino también de

los expedientes o sistemas de información; o en su caso, los someterá a un procedimiento de anonimización. Finalmente, se determina que para la supresión de los datos personales, el responsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de estos.

Los estándares señalan, además, que los países deberán determinar el plazo de conservación para garantizar los derechos y garantías de los titulares, y además dilucidando que los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifiquen su tratamiento o aquellas relacionadas con exigencias legales aplicables al responsable.

En suma, los elementos del principio de calidad son su exactitud, completitud, actualización, su tiempo de conservación y los procesos de eliminación.

iv. Finalidad

El numeral 17 de los estándares determina el principio de finalidad por el cual todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas. El responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquellas que motivaron el tratamiento original de estos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación. Es decir, los elementos sustanciales son la identificación de finalidades determinadas, explícitas y legítimas, y la prohibición de tratamiento para finalidades distintas a las autorizadas.

Finalmente, es destacable el precepto por el cual no se considerará incompatible con las finalidades iniciales y se faculta el tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, en favor del interés público. Este contenido no consta en la normativa latinoamericana vigente.

v. Seguridad

El principio de seguridad consta en el estándar 21; determina que el responsable establecerá y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Este principio es el que mayor desarrollo respecto de su contenido ha tenido en los últimos años. Dado que se ha establecido el principio de la seguridad demostrada, por el cual no solo es suficiente el contenido tradicional que establecía el establecimiento de las medidas citadas, sino que señala los siguientes elementos adicionales que permiten expresar un verdadero esfuerzo por garantizar seguridad:

a) *Criterios para determinar las medidas de seguridad aplicables:* El responsable considerará los siguientes factores: (a) El riesgo para los derechos y libertades de los titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión; (b) El estado de la técnica; (c) Los costos de aplicación; (d) La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles; (e) El alcance, contexto y las finalidades del tratamiento; (f) Las transferencias internacionales

de datos personales que se realicen o pretendan realizar; (g) El número de titulares; (h) Las posibles consecuencias que se derivarían de una vulneración para los titulares; (i) Las vulneraciones previas ocurridas en el tratamiento de datos personales.

b) *Acciones para implementar medidas de seguridad:* Por las cuales se garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica.

c) *Notificación de vulneraciones a la seguridad de los datos personales (estándar numero 22):* Por el cual, ocurrida una vulneración de seguridad, en cualquier fase del tratamiento, es decir cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental, notificará a la autoridad de control y a los titulares afectados dicho acontecimiento, sin dilación alguna, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de la vulneración de seguridad ocurrida, o bien, que esta no represente un riesgo para los derechos y las libertades de los titulares involucrados.

La citada notificación deberá estar redactada en un lenguaje claro y sencillo y contendrá, al menos, la siguiente información: (a) La naturaleza del incidente; (b) Los datos personales comprometidos; (c) Las acciones correctivas realizadas de forma inmediata; (d) Las recomendaciones al titular sobre las medidas que este pueda adoptar para proteger sus intereses; (e) Los medios disponibles al titular para obtener mayor información al respecto.

Además, el responsable documentará toda vulneración de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, de manera enunciativa más no limitativa, la fecha en que ocurrió; el motivo de la vulneración; los hechos relacionados con ella y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva, la cual estará a disposición de la autoridad de control.

vi. Consentimiento

Conforme señala el estándar numero 2 relativo a las definiciones, se entiende por consentimiento la manifestación de la voluntad, libre, específica, inequívoca e informada del titular por medio de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.

El estándar número 12 establece las condiciones necesarias para el consentimiento:

- Por medio de una declaración o una acción afirmativa clara.
- La posibilidad de que el titular podrá revocarlo en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos.

vii. Principio de legitimación

El principio de legitimación no ha sido recogido en la normativa latinoamericana, ya que en su lugar su contenido estaba descrito como parte de las excepciones al

consentimiento del titular. Aparece también en el *Proyecto de Ley Modelo sobre Protección de Datos Personales*, tomando en cuenta los estándares internacionales alcanzados en la materia. AG/RES. 2842 (XLIV-O/14).

La transformación de este principio se produce con la idea de que se conceptualice por sí mismo como aquellos criterios debidamente justificados y ponderados que motivan el tratamiento de datos personales en garantía del flujo de información que permita el desarrollo económico, político, social y cultural.

En ese sentido, en el precepto número 11 de los estándares se señala que por el principio de legitimación el responsable solo podrá tratar datos personales cuando se presente alguno de los supuestos siguientes:

a. El titular otorgue su consentimiento para una o varias finalidades específicas.
b. El tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato motivado de autoridad pública competente.
c. El tratamiento sea necesario para el ejercicio de facultades propias de las autoridades públicas o se realice en virtud de una disposición legal.
d. El tratamiento sea necesario para el reconocimiento o defensa de los derechos del titular ante una autoridad.
e. El tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el titular sea parte.
f. El tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable.
g. El tratamiento sea necesario para proteger intereses vitales del titular o de otra persona física.
h. El tratamiento sea necesario por razones de interés público previstas en la ley.
i. El tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, pero estos intereses no podrán prevalecer por sobre los intereses, los derechos o libertades fundamentales del titular, en particular de niños, niñas o adolescentes, por ser estos de atención prioritaria. Este análisis no será aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus competencias.
j. Constituye de interés legítimo el tratamiento de datos personales de contacto imprescindibles para la localización de personas físicas a los que el responsable presta sus servicios.

viii. Principio de licitud

Algunas de las legislaciones latinoamericanas sí reconocen el principio de licitud, como Argentina, Perú y Uruguay; así como las Directrices para la regulación de los archivos de datos personales informatizados. (Resolución 45/95 de la Asamblea General de las Naciones Unidas, de 14 de diciembre de 1990 y en el P*royecto de Ley Modelo sobre Protección de Datos Personales*, tomando en cuenta los estándares internacionales alcanzados en la materia. AG/RES. 2842 [XLIV-O/14]).

Este principio, conforme el estándar número 14, determina que el responsable tratará los datos personales con estricto apego y cumplimiento de lo dispuesto en la ley, el derecho internacional y los derechos y libertades de las personas.

Cabe anotar que el tratamiento de datos personales que realicen las autoridades públicas se sujetará a las facultades o atribuciones señaladas en la ley.

ix. Principio de lealtad

El estándar número 15 señala un principio que ha sido reconocido por República Dominicana, en el Proyecto de Ley Modelo sobre Protección de Datos Personales, tomando en cuenta los estándares internacionales alcanzados en la materia (AG/RES. 2842 [XLIV-O/14]). Asimismo, el contenido del principio de lealtad es parte del principio de legalidad en Perú y del principio de calidad en Uruguay y Argentina.

El principio de lealtad consiste en que el responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar estos a través de medios engañosos o fraudulentos.

Se aclara además que se considerarán desleales aquellos tratamientos de datos personales que den lugar a una discriminación injusta o arbitraria contra los titulares.

x. Principio de responsabilidad

El principio de responsabilidad consta en el precepto número 20 del estándar, el cual establece que el responsable y el encargado revisarán y evaluarán permanentemente los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidos, así como rendir cuentas sobre el tratamiento de datos personales a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo, con el objeto de medir su nivel de eficacia.

Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes: a) Destinar recursos para la instrumentación de programas y políticas de protección de datos personales; b) Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales; c) Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable; d) Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales; e) Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran; f) Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales; g) Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

El estándar recoge en el precepto 24 el derecho de los titulares de los datos de solicitar al responsable el acceso, rectificación, cancelación, oposición y portabilidad de los datos personales que le conciernen, denominados derecho ARCO. De forma que no es

necesario el ejercicio previo de otro, ni tampoco se impide el ejercicio de otro simultáneamente.

a. Derecho de acceso

El estándar número 24 establece como derecho de acceso el que tiene el titular de solicitar el acceso a sus datos personales que obren en posesión del responsable, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento.

b. Derecho de rectificación

En el estándar número 26 consta el derecho de rectificación, por el cual el titular tendrá el derecho a obtener del responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.

c. Derecho de oposición

En el estándar número 28 aparece el derecho de oposición, mediante el cual el titular podrá oponerse al tratamiento de sus datos personales cuando: a) Tenga una razón legítima derivada de su situación particular. b) El tratamiento de sus datos personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad. En el último caso, opera también cuando el titular expone su voluntad de que el responsable deje de usarlos.

d. Derecho de cancelación

En el estándar número 27, el derecho de cancelación señala que el titular tendrá derecho a solicitar la cancelación o supresión de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

El estándar número 29 señala el derecho a no ser objeto de decisiones individuales automatizadas que le produzcan efectos jurídicos o le afecten de manera significativa que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

El responsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los titulares por su origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, así como datos genéticos o datos biométricos.

No obstante, este derecho no procede cuando el tratamiento automatizado de datos personales sea necesario para la celebración o la ejecución de un contrato entre el titular y el responsable; esté autorizado por el derecho interno o se base en el consentimiento demostrable del titular. Cuando sea necesario para la relación contractual o el titular hubiere manifestado su consentimiento, tendrá derecho a obtener la intervención humana; recibir una explicación sobre la decisión tomada; expresar su punto de vista e impugnar la decisión.

f. Derecho de consulta al registro general de protección de datos personales

No consta en el estándar referencia a este derecho.

g. Derecho a indemnización por daños causados

El precepto número 44 señala el derecho de indemnización, mediante el cual se reconocerá el derecho que tiene el titular a ser indemnizado cuando hubiere sufrido daños y perjuicios, como consecuencia de una violación de su derecho a la protección de datos personales, para lo cual se sugiere que la normativa interna determine la autoridad competente para conocer de este tipo de acciones, así como los plazos, requerimientos y términos por medio de los cuales será indemnizado este, en caso de resultar procedente.

h. Derecho a la confidencialidad

En el estándar número 23 consta el principio de confidencialidad, mediante el cual el responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos; obligación que subsistirá aun después de finalizar sus relaciones con el titular.

i. Derecho al olvido digital

No consta en el estándar referencia a este derecho.

j. Spam

No consta en el estándar referencia a este derecho.

k. Derecho a la portabilidad de los datos personales

En el precepto número 30 del estándar aparece el derecho a la portabilidad de datos personales, que dispone que cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera. Además, señala que el titular podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros.

Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

l. Derecho a la limitación del tratamiento de los datos personales

El precepto número 31 del estándar señala que el titular tendrá derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el periodo que medie entre una solicitud de rectificación u oposición hasta su resolución por el responsable y cuando éstos sean innecesarios para el responsable, pero los necesite para formular una reclamación.

g) Procedimiento

En el precepto 32 del estándar se determina el procedimiento para el ejercicio de los derechos ARCO y el de portabilidad; para el efecto se determina la obligación del responsable de establecer medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad.

Los estándares sugieren que el procedimiento administrativo que provee cada Estado debe establecer los requerimientos, plazos, términos y condiciones en que los titulares podrán ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad.

Asimismo, los estándares proponen que las causales de improcedencia al ejercicio de los mismos consten de forma enunciativa más no limitativa y que al menos sean las siguientes: a) Cuando el tratamiento sea necesario para el cumplimiento de un objetivo importante de interés público; b) Cuando el tratamiento sea necesario para el ejercicio de las funciones propias de las autoridades públicas; c) Cuando el responsable acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del titular; d) Cuando el tratamiento sea necesario para el cumplimiento de una disposición legal; e) Cuando los datos personales sean necesarios para el mantenimiento o cumplimiento de una relación jurídica o contractual.

Ahora bien, ante la negativa del responsable los estándares reconocen el derecho que tiene el titular de inconformarse o impugnar las respuestas otorgadas por el responsable ante una solicitud de ejercicio de los derechos aludidos en el presente literal, o ante la falta de respuesta de este ante la autoridad de control y, en su caso, ante instancias judiciales.

h) Habeas data

No consta en los estándares referencia al *habeas data*.

a. Sujeto activo

No consta en los estándares referencia al *habeas data*.

b. *Sujetos pasivos u obligados*

No consta en los estándares referencia al *habeas data*.

c. *Derechos tutelados por el habeas data*

No consta en los estándares referencia al *habeas data*.

d. *Procedencia del habeas data*

No consta en los estándares referencia al *habeas data*.

e. *Procedimiento del habeas data*

No consta en los estándares referencia al *habeas data*.

i) Institucionalidad de protección

El estándar en el precepto número 42 señala que deben existir una o más autoridades de control y supervisión con plena autonomía. Estos pueden ser órganos unipersonales o pluripersonales; imparciales e independientes en sus potestades y actuaciones, ajenas a toda influencia externa, ya sea directa o indirecta, y no admitirán orden ni instrucción alguna. Las decisiones de las autoridades de control únicamente estarán sujetas al control jurisdiccional. Deberán contar con suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de esta, al igual que el ejercicio y respeto efectivo del derecho a la protección de datos personales, así como con suficientes recursos humanos.

El miembro o los miembros de los órganos de dirección de las autoridades de control deberán contar con la experiencia y aptitudes, en particular respecto al ámbito de protección de datos personales, necesarios para el cumplimiento de sus funciones y el ejercicio de sus potestades. Se nombrarán mediante un procedimiento transparente en virtud de la legislación nacional aplicable, y únicamente podrán ser removidos por causales graves establecidas en el derecho interno de cada Estado iberoamericano, conforme a las reglas del debido proceso.

j) Régimen sancionador

El precepto 43 de los estándares establecen el régimen de reclamaciones y de imposición de sanciones por el cual todo titular tendrá derecho a presentar su reclamación ante la autoridad de control, así como recurrir a la tutela judicial para hacer efectivos sus derechos.

El estándar sugiere que la legislación de cada Estado iberoamericano establezca un régimen que permita la adopción de medidas correctivas y sancionar las conductas que

contravengan lo dispuesto en las legislaciones nacionales correspondientes, indicando, al menos, el límite máximo y los criterios objetivos para fijar las correspondientes sanciones, a partir de la naturaleza, gravedad, duración de la infracción y sus consecuencias, así como las medidas implementadas por el responsable para garantizar el cumplimiento de sus obligaciones en la materia.

k) Ponderación del derecho a la protección de datos personales

Uno de los elementos que debe destacarse en los Estándares Iberoamericanos es el que consta en el precepto 7, acerca de la ponderación del derecho a la protección de datos personales, por el cual se puede exentar, en la normativa de cada Estado, el cumplimiento de los principios y derechos propios de la protección de datos personales, exclusivamente en la medida en que resulte necesario conciliar el derecho a la protección de datos personales con otros derechos y libertades fundamentales.

Esta exención deberá requerir de un ejercicio de ponderación con la finalidad de determinar la necesidad, idoneidad y proporcionalidad de la restricción o excepción conforme a las reglas y criterios de cada país.

l) Tratamiento de datos personales de niñas, niños y adolescentes

En el precepto 8 de los estándares propone una norma específica para el tratamiento de datos personales de niñas, niños y adolescentes, estableciendo la necesidad de privilegiar su protección, en virtud de su interés superior, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral.

En ese sentido, deberá promoverse la formación académica de las niñas, niños y adolescentes, el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales; así como el respeto de sus derechos y libertades.

Asimismo, en el precepto 13 de los estándares consta el consentimiento para el tratamiento de datos personales de niñas, niños y adolescentes, según el cual para la obtención del consentimiento de niñas, niños y adolescentes, el responsable obtendrá la autorización del titular de la patria potestad o tutela, conforme a lo dispuesto en las reglas de representación previstas en el derecho interno de cada Estado iberoamericano, o en su caso, solicitará directamente la autorización del menor de edad si el derecho interno ha establecido una edad mínima para que lo pueda otorgar directamente y sin representación alguna del titular de la patria potestad o tutela.

En ese caso, además, el responsable realizará esfuerzos razonables para verificar que el consentimiento fue otorgado por el titular de la patria potestad o tutela; o bien, por el menor directamente atendiendo a su edad de acuerdo con el derecho interno de cada Estado iberoamericano, teniendo en cuenta la tecnología disponible.

m) Tratamiento de datos personales de carácter sensible

El precepto 9 del Estándar Iberoamericano determina que el responsable no podrá tratar datos personales sensibles, salvo que se presente cualquiera de los siguientes supuestos:

a) Los mismos sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan su actuación; b) Se dé cumplimiento a un mandato legal; c) Se cuente con el consentimiento expreso y por escrito del titular; d) Sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros.

Los estándares proponen que la normativa de cada país deberá establecer excepciones, garantías y condiciones adicionales para asegurar el debido tratamiento de los datos personales sensibles, de conformidad con su derecho interno.

n) Transferencias internacionales de datos personales

Respecto de las transferencias de datos personales, el estándar 36 establece las reglas generales para las cuales un responsable y encargado pueden realizar transferencias internacionales de datos personales: a) El país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte del país transferente, conforme a la legislación nacional de este que resulte aplicable en la materia, o bien el país destinatario o varios sectores del mismo acrediten condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado; b) El exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y este, a su vez, acredite el cumplimiento de las condiciones mínimas y suficientes establecidas en la legislación nacional de cada Estado iberoamericano aplicable en la materia; c) El exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. La autoridad de control podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional de los Estados iberoamericanos aplicable en la materia; d) El exportador y destinatario adopten un esquema de autorregulación vinculante o un mecanismo de certificación aprobado, siempre y cuando este sea acorde con las disposiciones previstas en la legislación nacional del Estado iberoamericano aplicable en la materia, que está obligado a observar el exportador; e) La autoridad de control del Estado iberoamericano del país del exportador autorice la transferencia, en términos de la legislación nacional que resulte aplicable en la materia.

Finalmente, cada Estado bajo premisa establecida por los estándares iberoamericanos podrá establecer expresamente límites a las transferencias internacionales de categorías de datos personales por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros; así como por cuestiones de interés público.

o) Medidas proactivas en el tratamiento de datos personales

Criterio que amerita un nuevo capítulo en los estándares es el que consta en el precepto 37, relativo al reconocimiento de medidas proactivas, por las cuales se podrá reconocer y establecer medidas que promuevan el mejor cumplimiento de su legislación y coadyuven a fortalecer y elevar los controles de protección de datos personales implementados por el responsable, entre las cuales podrán encontrarse: privacidad por

diseño y por defecto, la implementación del oficial de protección de datos personales, los mecanismos de autorregulación y la evaluación de impacto a la protección de datos personales.

i. Privacidad por diseño y privacidad por defecto

El precepto 38 del estándar señala que el responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la ley. De tal manera que garantice que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado iberoamericano que le resulte aplicable. Esto con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de estos, sin la intervención del titular, a un número indeterminado de personas.

ii. Oficial de protección de datos personales

El precepto 39 del estándar señala que el responsable designará a un oficial de protección de datos personales o figura equivalente cuando: a) Sea una autoridad pública; b) Lleve a cabo tratamientos de datos personales que tengan por objeto una observación habitual y sistemática de la conducta del titular; c) Realice tratamientos de datos personales donde sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, considerando, las categorías de datos personales tratados, en especial cuando se trate de datos sensibles; las transferencias que se efectúen; el número de titulares; el alcance del tratamiento; las tecnologías de información utilizadas o las finalidades de estos, entre otras.

De oficio y aunque no se encuentre en una de las causas previstas, el responsable podrá designar a un oficial de protección de datos personales si así lo estima conveniente.

El responsable estará obligado a respaldar al oficial de protección de datos personales en el desempeño de sus funciones, facilitándole los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de estos.

El oficial de protección de datos personales tendrá, al menos, las funciones siguientes: a) Asesorar al responsable respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales; b) Coordinar, al interior de la organización del responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la legislación nacional del Estado iberoamericano que resulte aplicable en la materia; c) Supervisar al interior de la organización del responsable el cumplimiento de la legislación nacional del Estado iberoamericano que resulte aplicable en la materia.

iii. Mecanismos de autorregulación

El precepto 40 del estándar señala que el responsable podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, entre otros, contribuir a la correcta aplicación de la legislación y establecer procedimientos de resolución de conflictos entre el responsable y titular sin perjuicio de otros mecanismos que establezca la legislación nacional. En este sentido, se podrán desarrollar, entre otros, códigos deontológicos y sistemas de certificación y sus respectivos sellos de confianza que coadyuven a contribuir a los objetivos señalados en el presente numeral.

iv. Evaluación de impacto a la protección de datos personales

Conforme consta en el precepto 41 de los estándares iberoamericanos, cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa, a la implementación del mismo una evaluación del impacto a la protección de los datos personales. En este sentido, se prevé que la legislación nacional de los Estados iberoamericanos señalará los tratamientos que requieran de una evaluación de impacto a la protección de datos personales; el contenido de estas, los supuestos en que resulte procedente presentar el resultado ante la autoridad de control, así como los requerimientos de dicha presentación, entre otras cuestiones.

3. Conclusiones:

En un mundo globalizado y cada vez más tecnologizado, las actividades económicas, políticas y sociales de las personas se están realizando en Internet. Las tecnologías de la información y comunicación (TIC) tienen un impacto cada vez mayor en las relaciones nacionales e internacionales, en cuestiones cotidianas, profesionales, comerciales y de gobiernos.

En ese escenario, el dato personal juega un papel protagónico, ya que mediante tecnologías para transmisión, almacenamiento y procesamiento de datos, incluso de grandes volúmenes provenientes de diferentes tipos y fuentes, de naturaleza estructurada o desestructurada, se apuntalan las actividades en línea. Al mismo tiempo, se genera conocimiento para la toma de decisiones, cada vez más especializada, rápida y eficiente; se determinan patrones y tendencias; se proporcionan medios para un acercamiento directo y efectivo a los consumidores y al ciudadano, se crean nuevos bienes y servicios públicos y privados o se mejoran los existentes. Las distintas partes interesadas, particulares, organismos, empresas, gobiernos se interrelacionan y generan nuevos modelos de negocio y de participación que permiten un espacio de interacción para el desarrollo tecnológico, la competitividad y la innovación.

Asimismo, el acceso universal a tecnologías de la información y comunicación facilitan el debate, la construcción de un foro mundial y la democracia deliberativa; pues permite que se escuchen todas las voces, en especial de aquellas que buscan, en la diferencia, romper la filtración de la información generada desde el poder tecnológico o económico

al "amplificar la voz de los/las activistas de derechos humanos y contribuir a desvelar los abusos".[1134]

Es la propia persona la que recibe beneficios constantes en sus interrelaciones con proveedores, empresas, Estados e incluso con otros pares, lo que ha naturalizado el intercambio de su información, pues su percepción de acceso, accesibilidad, disponibilidad, velocidad, que antes se consideraban un privilegio, paulatinamente se van convirtiendo en el estándar. A tal punto que, ahora no se conciben servicios públicos o privados, aplicaciones y plataformas que no briden este nivel de satisfacción al usuario. Todo ello potenciado por la penetración de la comunicación móvil, de los microcomponentes, la geolocalización, el internet de las cosas y más tecnología que habilita la hiperconexión en tiempo real.

El ser humano es el centro de este modelo de interacción, pues es su información la que nutre este ecosistema digital. Sin embargo, existen riesgos que se presentan en el momento del uso de las comunicaciones digitales y el tratamiento de los datos personales. Problemáticas que van desde cuestiones administrativas, técnicas, tecnológicas, hasta relativas a posibles transgresiones a libertades individuales y derechos fundamentales. Por ejemplo, inseguridad, pérdida o destrucción, alteración, manipulación de datos personales, transmisión o tratamiento inadecuado o no consentido, robos de identidad, discriminación producida por perfiles o de procesos automatizados, disminución del acceso universal a internet, alteración de la neutralidad de la red, afectación a la libertad de pensamiento y expresión o la invasión de la intimidad o la privacidad, a través de la vigilancia o la interceptación electrónica o el almacenamiento masivo de datos, entre otros.

Cada país, dependiendo de sus propias características y condiciones, ha establecido distintas formas de abordaje de la realidad descrita. Como estudiamos en el capítulo II de este trabajo de investigación, Europa lo ha hecho desde el reconocimiento de un derecho fundamental denominado "protección de los datos personales", mientras que otras regiones lo hacen desde otro derecho o criterio como la *privacy*. En cualquier caso, es importante tratar de entender y valorar desde cada perspectiva, las realidades y condiciones propias de cada normativa y región, y comprender cómo se han manejado estos temas en las diversas realidades mundiales.

Desde el modelo europeo, la primera aproximación a la protección de las personas ante las posibles vulneraciones que las tecnologías de la información y comunicación se hizo desde el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, que a nivel internacional es el único instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos.

Posteriormente, el modelo europeo nos muestra, como siguiente paso evolutivo, la construcción de un nuevo derecho, el de la protección de los datos personales, a través de la Decisión 45/95. En dicha normativa, Europa reconoce y desarrolla un nuevo derecho autónomo y diferente de la intimidad (esfera íntima: familiar o personal) y de la

[1134] NACIONES UNIDAS DERECHOS HUMANOS OFICINA EL ALTO COMISIONADO, "El derecho a la privacidad en la era digital", accedido el 29 de septiembre de 2019, https://www.ohchr.org/SP/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

privacy (esfera íntima: familiar, personal o social), como se lo conoce en el derecho anglosajon.

Esta clara distinción entre derechos se evidencia en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea de 2000, en los que se consagran los derechos a la vida privada y a la protección de datos, respectivamente. Además, en el artículo 16 del Tratado de Funcionamiento de la Unión Europea de 2010 se reconoce expresamente, el derecho a la protección de datos personales.

Finalmente, el Parlamento Europeo y el Consejo de Europa de 27 de abril de 2016 dictaron el Reglamento General de Protección de Datos. Norma por la cual las personas físicas pueden ejercer los derechos a la autodeterminación informativa y protección de datos personales: esto es acceso, rectificación, supresión, oposición, portabilidad, entre otros. Así como, recoge una serie de principios y obligaciones que los responsables de tratamiento deben cumplir para realizar un tratamiento adecuado de los datos personales garante de derechos fundamentales.

En el presente capítulo se ha revisado los principales instrumentos internacionales, que tienen repercusión en los países latinoamericanos y que hacen referencia a la privacidad o a la protección de datos personales. Dicha normativa desarrolla la garantía constitucional del *habeas data,* cuyo origen es portugués pero que ha sido ampliamente implementado en las normativas nacionales de la región. El *habeas data* es la garantía constitucional que viabiliza la protección a la vida privada de las personas. Pero que además, faculta la posibilidad de tomar decisiones, mantener un espacio de tranquilidad, reserva sobre ciertos aspectos de la vida privada y controlar la difusión de información personal. Al respecto, la Corte Interamericana de derechos humanos ha dispuesto que a través de la privacidad se protege al menos cuatro bienes jurídicos: la intimidad; la autodeterminación informativa; el secreto y la prohibición de divulgación de datos personales sin autorización del titular; y, la propia imagen. De lo dicho, la definición, el alcance y desarrollo de la figura del *habeas data* se aliena y complementa en mayor medida con el derecho a la protección de datos personales, aunque sigue atado limitadamente a la vida privada. Asimismo, Latinoamérica ha reconocido la insuficiencia de su modelo constitucionalista asociado al *habeas data* y ha adoptado mayoritariamente el modelo continental, que es precisamente aquel que reconoce la existencia de un derecho fundamental diferente a la *privacy* y que involucra un mayor estándar de protección.

Respecto de los 21 informes anuales de la Relatoría para la Libertad de Expresión, se colige que, si bien su contenido hace referencia directa al ejercicio de la libertad de expresión, sin embargo no se distingue entre privacidad e intimidad a lo sumo se hace referencia al *habeas data* y no se reconoce la existencia del derecho autónomo e independiente denominado protección de datos personales. Ahora bien, el mayor avance de estas relatorías es el reconocimiento de que la vigilancia e interceptación, el uso inadecuado de los datos, así como la recolección y retención masiva de datos personales, incluidos los metadatos telefónicos y electrónicos, afectan la privacidad de los individuos, lo que tiene incide directa en la libertad de expresión. Esto se debe a que, el ciudadano solo si se siente libre de amedrentamientos y de represalias, cuando percibe que no es supervisado o vigilado, de forma directa o indirecta por parte del Estado o de particulares puede ejercer su derecho a ser informado, a desarrollar su libre

pensamiento, a expresar su opinión en el foro público, incluso de manera anónima; así como a convocar a movilizaciones sociales.

Pese al avance de los instrumentos internacionales estudiados, tanto de los informes de las Relatorías a la Libertad de Expresión, de las sentencias dictadas por la Corte Interamericana de Derechos Humanos y de las resoluciones de la Organización de Estados Americanos se colige que, aún no se reconoce, el derecho a la protección de datos personales sino que se concibe únicamente el derecho a una vida privada. Todo ello, en aplicación de lo dispuesto en el artículo 11 de la Convención Americana de Derechos Humanos que determina la prohibición de que terceros o el Estado realicen injerencias arbitrarias o abusivas en la vida privada, la familia, el domicilio, la correspondencia, o de realizar ataques ilegales a la honra o reputación de un individuo.

Es decir, desde los instrumentos internacionales e incluso de las Resoluciones de Naciones Unidas reconocen solamente a la privacidad como derecho fundamental. De esta forma, para este organismo, la protección de datos personales se limita a ser vista como un mecanismo, herramienta, estrategia o política que debe ser puesta en práctica para garantizar la privacidad de las personas en la era digital. Anotándose que, no es suficiente que la privacidad esté recogida en políticas de ciberseguridad, porque no se trata de un enfoque de seguridad de los datos personales sino de un sistema integral de protección que determine principios, derechos y obligaciones.

Las resoluciones de Naciones Unidas, relativas a regulación de archivos de datos personales automatizados, la promoción, protección y disfrute de los derechos humanos en Internet, también se acotan en el derecho a la privacidad en la era digital. Dichos instrumentos, en los últimos años reconocen la problemática de la vulneración de los derechos humanos en los entornos digitales y establecen contenidos, criterios y recomendaciones a los países para prevenir y erradicar toda forma de violencia digital.

Ahora bien, el modelo de la *privacy*, con el cual los países que pertenecen al *common law* abordan el tema de los datos personales, está en crisis. Por cuanto se considera que este derecho que se activa solo si se ha producido una exposición o daño a un titular, es decir no tiene efecto preventivo porque no regula el adecuado manejo del dato personal sino la afectación a la privacidad o intimidad de los titulares de los datos. Además, representa un sistema fragmentado de protección por cuanto se regula por sectores sin que exista una única visión que evite vacíos de aplicación o interpretación. Tanto más que, los responsables de tratamiento públicos no se encuentran regulados sino a través de normas de excepción que habilitan, de una manera amplia, motivados en cuestiones de orden público y seguridad nacional, el tratamiento de datos personales. Asimismo, su campo de aplicación es acotado a los datos considerados sensibles, cuando la protección integral determina que es suficiente que se trate de datos personales sin cualificación adicional, toda vez que, sobre cualquier dato, fragmento de dato o incluso dato inocuo, con tal que sea dato personal, el titular tiene derecho a la autodeterminación informativa

Sin embargo, los recientes sucesos asociados a eventos de manipulación de masas con la intención de direccionar la decisión de voto de los ciudadanos americanos, por medio de la obtención de datos de millones de sus usuarios, y la elaboración de perfiles de personalidad mediante el acceso a la plataforma Facebook, demuestra que en el estado

actual de la técnica debe reconocer, al menos, que la necesidad de reforzar la privacidad aumentará aún más.

Entonces, es evidente que las transgresiones ahora son exponenciales porque ya no se trata de una afectación limitada a un individuo específico en su entorno privado, sino que, como ocurre en el caso Facebook, pueden llegar a afectar a una masa de personas, que completamente ajenas e ignorantes del inadecuado manejo de sus datos personales pueden ser manipuladas, de tal forma que incluso se puedan estar afectando las bases mismas de la sociedad civilizada, esto es, la democracia misma.

De lo citado, el Internet es un adelanto tecnológico que debe propiciar una mejor calidad de vida del individuo. Para que esto sea posible es necesario que los derechos humanos puedan ser protegidos en estos entornos tecnológicos. De ahí que, se evidencia la necesidad de analizar nuevas facetas o enfoques digitales para completar y añadir nuevas características, condiciones o elementos esenciales a los derechos existentes. Pero además, debemos comprender que aparecerán otros derechos que tienen su origen directo en el desarrollo tecnológico y que irán completando el catálogo de derechos digitales, del que ahora las personas gozamos en garantía de que nuestra dignidad ya no es solo física sino virtual y que es indispensable una protección integral.

De lo señalado, es indiscutible la necesidad de normativa de aplicación universal a través del derecho internacional de los derechos humanos. Son varios los que deben desarrollarse, ampliarse y generalizarse, entre ellos: la privacidad y el derecho a la protección de datos personales, así como en el derecho de acceso universal a internet, la libertad de expresión en la era digital, la educación digital, la neutralidad de la red, la neutralidad tecnológica, el anonimato, el cifrado, la ciberseguridad, entre otros. Y aunque, cada país, tiene propias características que condicionan su desarrollo económico, político y social es a través de la universalización de los derechos humanos que se puede construir un sistema homogéneo de protección que viabilice un estándar similar de protección en el mundo.

Por eso, es esencial encontrar un enfoque que garanticen el fin último de toda regulación: la protección integral del ser humano. Cualquier modelo que no establezca un estándar mínimo de protección pone en riesgo a la persona. Por ello, el estándar más alto, que, actualmente, consiste en el reconocimiento del derecho a la protección de datos personales pasa a ser el nivel deseado, en la medida en la que de esta manera se evita dejar espacios de desprotección, pues el uso inadecuado de datos personales no solo afecta la privacidad de las personas sino que impide el ejercicio de otros derechos o incluso puede colocar al titular en situación de discriminación o de valoraciones equivocadas, porque sus datos personales se convierten en sus antecedentes. Asimismo, las nuevas tecnologías siguen desarrollándose de manera estrepitosa y no existe manera de prever o anticipar sus repercusiones, por lo que, la única actitud responsable es reconocer la existencia de este derecho autónomo e independiente, que incluso debe fortalecerse paulatinamente.

El considerar a la protección de datos personales como un derecho de la persona, es adoptar una visión garantista asociada a la dignidad e integridad humana. Su contenido deberá seguir enriqueciéndose y, además será indispensable ir apuntalándolo a través de varios mecanismos de salvaguarda del individuo en la era digital.

El progreso vertiginoso de la tecnología vuelve urgente la generación inmediata de marcos normativos obligatorios de carácter internacional, pero también regional, nacional y local; así como, de estándares o guías organizativas y técnicas que se apliquen en los distintos sectores o ámbitos públicos o privados.

Debido a la transnacionalidad del tratamiento y las consecuencias extraterritoriales del uso inadecuado de las Tic y de los datos personales dichas normativas deben estar armonizadas, a través de convenios o tratados comunitarios, o de aplicación regional, que permitan, a la usanza del modelo europeo, dotar al titular del dato personal de una protección integral en los actuales entornos globalizados.

En el año 2015, el Consejo de Derechos Humanos creó el mandato del Relator Especial sobre el derecho a la privacidad, para que identifique las principales transgresiones a este derecho y establezca recomendaciones para su salvaguarda.

Asimismo, la Organización de los Estados Americanos dicta recomendaciones que buscan establecer criterios que deben tomarse en cuenta en la generación o reforma de la normativa de la región que viabilice la protección del individuo y sus datos personales. Destacándose la elaboración de la Ley Modelo, que si bien representa una iniciativa interesante al establecer una Guía Legislativa; sin embargo, su contenido solo refleja mínimos esenciales de protección, por lo que se consideran un nivel inferior de protección respecto de otros modelos como el europeo, al cual se considera el estándar más alto de protección.

Aún más, esta iniciativa armonizadora, no ha logrado calar en la región, puede ser debido a que los países en sus normas internas, a excepción de unos pocos países, tienen estándares de protección más garantistas, alineados al modelo europeo, por lo que esta Ley Modelo pudiera resultar insuficiente. Ya que, muchos países reconocen a nivel constitucional y legal el derecho a la protección de datos personales, diferenciándolo del derecho a la vida privada, por ejemplo.

Asimismo, la Red Iberoamericana de Protección de Datos Personales, el 20 de junio de 2017, ha dictado los Estándares de Protección de Datos de los Estados Iberoamericanos, como un intento de promover la actualización de normativas existentes, impulsar la cooperación efectiva y fortalecer los procesos regulatorios de la región.

Ahora bien, el instrumento que sin duda ha motivado la aprobación de normativas locales (Brasil, Panamá, Ecuador) es el Reglamento General de Protección de Datos Personales, dictado por la Unión Europea que ha visibilizado la problemática del avance desenfrenado de la tecnología, el uso masivo de los datos personales y la necesidad de una real, práctica y eficiente regulación que viabilice su protección

Es evidente la necesidad de dictar normativas internacionales como tratados o convenios entre los Estados americanos. Incluso propiciando la generación de una normativa comunitaria de carácter vinculante tal como ocurre en Europa con el RGPD. Ya que, solo desde la unión de las naciones se puede contrarrestar el poder de las grandes plataformas y corporaciones transnacionales.

Por el momento, una iniciativa válida llevada a cabo por Argentina[1135], Uruguay[1136] y México[1137] y que debiera ser emulada por otros países de la región, es la adhesión al Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal. Asimismo, y respecto del RGPD se ha declarado a Argentina como primer país[1138], y al Uruguay[1139] como el segundo país adecuado para el tratamiento de datos personales.

Finalmente, tanto de las recomendaciones de la OEA como de las Naciones Unidas se establecen que para la protección de los derechos humanos en la era digital se debe incentivar a empresas a adoptar un modelo responsable y proactivo de acción, que no solo lo proyecte a cumplir con la normativa local sino que analice el riesgo, lo prevenga, lo mitigue y de ser el caso repare el daño causado. Todo desde la perspectiva no solo del cumplimiento de las disposiciones normativas sino de la generación de una confianza digital que viabilice la generación de mayores y mejores modelos de negocio, que lo otorguen una ventaja comparativa, por la transparencia y buena reputación que el manejo adecuado de los datos personales puede otorgarle y que repercute

1135 El 25 de febrero de 2019 Argentina ratifica el Convenio Nº108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, adoptado en Estrasburgo, y el Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos adoptado en Estrasburgo, el 8 de noviembre de 2001. Dicha normativa entró en vigencia el 01 de junio de 2019, de esta forma Argentina es el tercer país latinoamericano en ratificar este Convenio.

1136 Primer país de Latinoamérica en firmar este Convenio. El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, "Ley No 19.030 aprobación del Convenio No 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos", República Oriental del Uruguay, Poder Legislativo, 2012, accedido 25 de agosto de 2017, https://parlamento.gub.uy/documentosyleyes/leyes?Ly_Nro=19030&Ly_fechaDePromulgacion%5Bmin%5D%5Bdate%5D=&Ly_fechaDePromulgacion%5Bmax%5D%5Bdate%5D=&Ltemas=&tipoBusqueda=T&Searchtext=.

1137 De otro lado, el 28 de junio de 2018 México ratifica el Convenio Nº108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, adoptado en Estrasburgo, y el Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos adoptado en Estrasburgo, el 8 de noviembre de 2001. Dicha normativa entró en vigencia el 01 de octubre de 2018, de esta manera México es el segundo país latinoamericano en firmar este Convenio.

1138 "Decisión 2003/490/CE, de 30 de junio de 2003, de la Comisión de la Unión Europea, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina (Texto pertinente a efectos del EEE)", *EUR-Lex - 32003D0490 - EN - EUR-Lex*, 2003, accedido 25 de agosto de 2017, http://eur-lex.europa.eu/legal-content/ES/TXT/?toc=OJ%3AL%3A2003%3A168%3ATOC&uri=uriserv%3AOJ.L_.2003.168.01.0019.01.SPA.

1139 La Comisión Europea, "Decisión de Ejecución 2012/484/UE, de 21 de agosto de 2012, de la Comisión de la Unión Europea de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales [notificada con el número C(2012) 5704] (Texto pertinente a efectos del EEE) (2012/484/UE)", *EUR-Lex*, accedido 25 de agosto de 2017, http://eur-lex.europa.eu/legal-content/ES/TXT/?toc=OJ%3AL%3A2012%3A227%3ATOC&uri=uriserv%3AOJ.L_.2012.227.01.0011.01.SPA.

estructuralmente en la lealtad y transparentar en las relaciones empresa - consumidor, Estado - ciudadano.

Dichos organismos de forma unívoca consideran que para lograr una efectiva protección de las personas, su privacidad y sus datos personales es necesaria la creación de una institución independiente, imparcial con autonomía administrativa y financiera que pueda regular al poder del Estado, al de las empresas nacionales, a los organismos internacionales y que, a través de la coordinación internacional con otros instituciones similares, permita controlar también a las plataformas trasnacionales.

Se puede concluir que, desde la ONU y la OEA la *privacy* se encuentra adoptando o acoplando otros contenidos que lo alienan hacia el derecho a la protección de datos personales. Lo señalado se evidencia cuando, además de reconocer la obligación de abstención de personas públicas o privadas de acceder o difundir aspectos de la esfera privada de un individuo, las recomendaciones de los citado organismos, otorgan al titular derechos sobre la exposición injustificada de su información. En este sentido, se amplía a la *privacy* desde la perspectiva de que el titular tiene derecho a conocer qué tipo de información se está recopilando, a expresarle a una empresa que no comparta ni venda su información personal, a que sus datos se encuentren almacenados en entornos técnicos y organizativos seguros, entre otros. En suma, una serie de derechos que incluso aparecen en la denominada *Data Protection Act.* Todo lo cual demuestran que respecto del tratamiento de datos personales existen las mismas preocupaciones a nivel mundial, pero diferente nivel de respuesta ante estas problemáticas idénticas, por lo que los distintos sistemas de protección paulatinamente irán acercándose.

De lo visto, resulta inminente, la generación de un modelo mundial que adapte las distintas visiones, incluso provenientes de los sistemas jurídicos de cada región y que habiliten un intercambio consensuado, respetuoso de los derechos fundamentales que establezcan mecanismos y procedimientos reales, efectivos y expeditos para garantizar los derechos de las personas en Internet.

Lo importante es no perder el horizonte, esto es que la protección de los datos personales debe estar centrada en la persona y sus derechos. Sin descuidar, que la armonización de la normativa es necesaria para facilitar el desarrollo económico regional, la libre competencia, la igualdad, la interoperabilidad mundial, el libre flujo de información, la innovación, el emprendimiento, el acceso universal a las Tic y al internet, todo ello, en aras de ampliar y mejorar la economía digital; en suma de cumplir de las objetivos de desarrollo sostenible.

CAPÍTULO IV

El DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL CONTEXTO LATINOAMERICANO

1. Reconocimiento del derecho a la protección de datos en Latinoamérica

Las tecnologías de la información y comunicación (TIC) usadas en el común de las actividades diarias, la interconexión que permite una interrelación inmediata, *online*, solo pueden manifestarse en una sociedad luego de ingentes inversiones económicas en infraestructura tecnológica; de ahí que esta es una de las causas por las cuales la sociedad red[1140] llega a Latinoamérica más tardíamente que a Europa y Estados Unidos, por ejemplo.

En aquellas cuestiones nuevas, como las relativas a la incorporación de las TIC, Europa y Norteamérica son referentes que influyen directamente en los derechos locales y en la legislación de los países latinoamericanos. En el caso de la protección de datos, Latinoamérica recibe esta influencia y adopta una especie de posición intermedia entre la idea anglosajona de un sistema de *common law* enfocado en la *privacy*; y las iniciativas europeas en las que el "problema no es la herramienta sino la defensa integral de los datos personales"[1141].

Entonces, se puede colegir que, en un primer acercamiento, el derecho a la protección de datos personales en Latinoamérica no fue concebido como un derecho fundamental propio y distinto, de origen jurisprudencial, a la sazón de lo ocurrido en Europa.

Se comparte con la doctrina mayoritaria europea y anglosajona la conceptualización de ser un derecho dedicado al "amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad"[1142]. Sin embargo, el inicial abordaje latinoamericano no provino de identificarlo como derecho fundamental, sino como un mecanismo de tutela o garantía constitucional denominado *habeas data*.

Al igual que ocurrió en el continente europeo, el derecho a la protección de datos tuvo sus antecedentes inmediatos en el derecho a la intimidad a tal punto de construir un nuevo derecho basado en la autodeterminación informativa. Posteriormente, varios países logran su diferenciación, y por ende su autonomía e independencia. Asimismo, el *habeas data* se limitaba a ser un mecanismo de protección exclusivamente del derecho a la intimidad y, después, amplió su rango de amparo a otros derechos fundamentales.

Latinoamérica se aleja de la visión anglosajona, que protege la *privacy* de las personas mediante normativas básicas como *Privacy Act*, o de regulaciones propias del libre mercado y de la autonomía de la voluntad de las partes. Estos elementos no aparecen en normativas latinoamericanas más apegas a una regulación de corte constitucional por medio de la tutela del *habeas data* o, incluso de leyes específicas sobre protección de datos personales.

[1140] M. CASTELLS Y F. MUÑOZ DE BUSTILLO, *La sociedad red: Una visión global* (Madrid: Alianza Editorial, S.A., 2013).
[1141] O. GOZAN, *Hábeas Data, protección de datos personales* (Buenos Aires: Rubinzal-Culzoni Editores, 2001), 9.
[1142] M. A. DAVARA RODRÍGUEZ, *Manual de Derecho Informático*, 47.

En varios ordenamientos jurídicos, entre ellos el ecuatoriano, se considera al "hábeas data como derecho y no, como preferimos, por resultar más propio y fiel a su concepción originaria, como acción procesal constitucional"[1143]. Un derecho que coincide en su totalidad con el contenido que plantea la autodeterminación informativa, pero al mismo tiempo significa en sí mismo una acción conducente a garantizar no solo este derecho fundamental sino otros relacionados con él como la intimidad, el honor, la identidad, la información, etc.[1144]

La evolución constitucional del derecho a la protección de datos en Latinoamérica tiene mediante la figura del *habeas data* una deconstrucción práctica que permite al ciudadano su ejercicio.

En efecto, los países latinoamericanos, en su mayoría, han ido incorporando normas constitucionales relativas a la protección de datos por medio del *habeas data*, de la cual coexisten múltiples variantes, ya sea reconocido como derecho, como acción procesal constitucional autónoma o como uno de los elementos que integra una garantía como el amparo.

En sentido contrario, muchos países latinoamericanos han omitido consagrar el derecho a la protección de datos personales por considerar que la acción constitucional constituye en sí misma el reconocimiento de este derecho. Analizaremos si esta postura resulta ser acertada o si es necesario cuestionarse acerca de esta forma de protección, ya que el objetivo final es la eficacia del derecho a la protección de datos personales.

Palazzi sostiene que el "*habeas data* representa apenas un intento dirigido a corregir distorsiones extremas del proceso comunicativo informático, ya que de un lado reduce la invisibilidad de los gestores o titulares de los bancos de datos porque los hace sujetos de una responsabilidad clara ante el titular de los mismos, y por el otro lado, permite a las personas en cierta medida adquirir conciencia de la transparencia externa e incluso de la importancia que tiene su propia información personal"[1145].

Además, pese a que muchos países han consagrado el *habeas data* como una garantía constitucional que permite el ejercicio de los ciudadanos a controlar sus datos, no necesariamente han desarrollado normativa legal que regule aspectos como su ámbito, principios, responsabilidad de los titulares de los ficheros, niveles de seguridad, infracciones, sanciones, organismos encargados de control específico, entre otros.

A continuación se identificarán los antecedentes internacionales del derecho a la protección de datos personales con referencia a Latinoamérica para determinar la configuración particular en este lado del mundo y diferenciarla de otros regímenes de protección existentes. No se hará mención al régimen previsto en Europa ni a los antecedentes que en este continente dieron nacimiento al derecho, aunque sin duda son de gran importancia porque ya fueron analizados en el segundo capítulo de esta investigación. Tampoco se hará referencia a Estados Unidos, por tratarse de un sistema diferente basado en el *common law*.

[1143] O. PUCCINELLI , "Tipos y subtipos de hábeas data en América Latina".
[1144] Ibíd.
[1145] P. A. PALAZZI, *La Transmisión Internacional de Datos Personales y la Protección de la Privacidad Argentina, América Latina, Estados Unidos y la Unión Europea* (Buenos Aires: Ad Hoc), 99 y s.

2. Análisis de la normativa latinoamericana a la luz de los elementos que son parte del contenido esencial del derecho a la protección de datos

La protección de datos personales en América Latina tiene un proceso de conformación paulatina del derecho. Sin duda, para su incorporación en las normativas constitucionales y legales de la región, ha sido fundamental la influencia de los instrumentos internacionales anteriormente analizados.

Se puede identificar sus antecedentes más inmediatos en derechos conexos como la intimidad, la limitación a la libertad de expresión, la protección al honor y a la buena reputación. Pero, es aún más importante el posicionamiento de la figura constitucional del *habeas data* como respuesta latinoamericana a proteger a las personas de las transgresiones producidas por la tecnología y la informática, no necesariamente asociada únicamente al derecho a la protección de datos personales, sino como tutela constitucional de otros derechos fundamentales que pudieran ser quebrantados en esta nueva esfera en la que se desenvuelve el ser humano: la informática, lo virtual, lo digital.

A continuación se realizará una revisión cronológica de los países que han incorporado algún tipo de legislación que proteja la intimidad, la privacidad, los datos personales en cualesquiera de sus formas de protección, esto es mediante la consagración de derechos fundamentales, acciones constitucionales propias como el *habeas data*, acciones constitucionales tradicionales como el amparo y la tutela, normas legales específicas, generales o sectoriales, entre otros. El estudio será de carácter cronológico, de tal forma que se analizará primero aquellos países que incorporaron cualquier forma de protección antes descrita en sus respectivas Constituciones y las vigentes a la fecha de corte de investigación.

2.1 Guatemala (1985)

La primera Constitución latinoamericana que incluyó elementos del derecho a la protección de datos personales es la guatemalteca de 1985 (antes artículo 35), reformada en 1993 que textualmente expone: "Art. 31. Es el derecho de toda persona de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos"[1146].

La primera aproximación que tenemos de este derecho en Latinoamérica se presenta desde una perspectiva instrumental; dicho de otro modo, un derecho se convierte en medio para garantizar la vigencia de otros derechos. En este caso, la norma citada, mediante la protección de datos personales, protege las libertades individuales, en especial la libertad de ideología como garantía de democracia de un Estado.

[1146] Guatemala, *Constitución Política de la República de Guatemala* [1985], Biblioteca Virtual Miguel de Cervantes, accedido 11 de mayo de 2017, http://www.cervantesvirtual.com/obra-visor/constitucion-politica-de-la-republica-de-guatemala-de-1985/html/.

El artículo señalado delimita el derecho al conocimiento y acceso a los datos personales y no hace referencia a la autodeterminación informativa; menciona únicamente ficheros estatales, y por lo tanto, el Estado es el único que figura responsable del tratamiento de datos personales. Prohíbe de forma expresa recabar datos de carácter político, dejando de lado otros datos de carácter sensible. Esta norma fue dictada en el inicio de la era democrática de Guatemala, luego de varios gobiernos militares y presidentes sin designación popular. Su diseño pretende establecer una limitación al poder. De ahí, el claro direccionamiento de su contenido a las actuaciones del Estado, el cual con el pretexto de garantizar seguridad, elaboraba ficheros de datos personales con la finalidad de identificar a personas, grupos e ideas opositoras al régimen de turno.

Esta forma de reconocimiento del derecho es lo que se considera una protección de primera generación. Entendida como aquella en la que el derecho a la protección de datos se establece con un contenido limitado a la protección del individuo frente a las posibles transgresiones realizadas por el Estado.

El 23 de septiembre de 2008, mediante Decreto 57-2008, se promulgó la Ley de Acceso a la Información Pública, en cuyo texto constan varios artículos que desarrollan ciertas definiciones que ayudan a dar forma al derecho a la protección de datos personales, sobre todo respecto a la naturaleza del dato personal, el dato sensible, el dato personal sensible, el *habeas data*, el acceso a la información pública, la información confidencial y la información pública, la información reservada, la máxima publicidad y la seguridad nacional, entre otras.

Finalmente, conforme señala Antonio Troncoso Regaida, en Guatemala existe normativa de carácter sectorial[1147] que ayuda a mejorar la protección de datos personales como:

a) Ley de Derecho de Autor y Derechos Conexos Decreto 33-98, que al establecer el régimen jurídico de las bases de datos, en el artículo 35 señala que la protección desde el derecho de autor no se extenderá a los datos o material contenido en ellas.

b) Decreto 006-2003 del Congreso de la República, Ley de Protección al Consumidor y Usuario, en la que constan la obligación del consumidor o usuario de entregar información relacionada con créditos de consumo para la adquisición de un bien o servicio, conforme el artículo 27 de la citada ley.

Ninguna de estas dos referencias legales contribuye a determinar el contenido esencial del derecho a la protección de datos en Guatemala.

a) Ámbito: Registros o ficheros públicos

Del análisis de la versión constitucional sobre *habeas data* podemos colegir que en Guatemala solo se protege la información personal que conste en registros públicos.

[1147] A. TRONCOSO REIGADA, "El desarrollo de la protección de datos personales en iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de protección de datos a nivel internacional", *Revista Internacional de Protección de Datos Personales*, n.º 1 (2012): 12, accedido 6 de mayo de 2017, https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/10_Antonio-troncoso_FINAL.pdf.

Esta exégesis se corrobora con el contenido del artículo 1 de la citada ley que al señalar su objeto expresamente manifiesta:

> Artículo1. La presente ley tiene por objeto: [...] 2. Garantizar a toda persona individual el derecho a conocer y proteger los datos personales de lo que de ella conste en archivos estatales, así como de las actualizaciones de los mismos…

Ahora bien, la Corte de Constitucionalidad de Guatemala, en Expediente 1356-2006, de 11 de octubre de 2006, señala expresamente que:

> En Guatemala no existe tal regulación, y en tanto no la haya, para no incurrir en situaciones *legibus solutus*, a criterio de esta Corte toda comercialización de información de datos de una persona debe estar sujeta a que esa información fuera proporcionada voluntariamente por la persona, cuyos datos serán objeto de comercialización; y que al momento de obtenerse, se le haya garantizado a dicha persona los derechos de actualización, rectificación, confidencialidad y exclusión antes citados, como una forma de resguardar los derechos fundamentales a su intimidad personal, privacidad y honor.[1148]
>
> De tal forma que garantiza los datos personales contenidos en ficheros regentados por entes privados desde otros derechos fundamentales como la intimidad personal, la privacidad y el honor en ausencia de un adecuado nivel de cobertura del derecho a la protección de datos.

b) Naturaleza del dato

El artículo 35 de la Constitución de Guatemala referido al derecho a la protección de datos personales, aunque en una versión limitada al ámbito público, hace alusión a archivos, fichas o cualquier otra forma de registros estatales; mientras que el artículo 4 de la Ley de Acceso a la Información Pública señala a la información contenida en registros, archivos, fichas, bancos, o cualquier otra forma de almacenamiento. Vemos una coincidencia en la utilización de términos que de manera implícita permiten señalar que la protección se refiere a la información de una persona. En este caso, las normas en cuestión hacen referencia a formatos o soportes en las que esta información está almacenada más que a su vinculación a determinada o determinable persona. Además, la norma está redactada de tal manera que no queda claro si la protección incluye un ámbito físico y otro electrónico, y en virtud de una interpretación progresiva de derechos se entiende que se protegen los dos medios.

Ahora bien, el artículo 9 de la Ley de Acceso a la Información Pública, cuando realiza las definiciones aplicables al contenido de la misma, define datos personales como aquellos relativos a cualquier información concerniente a personas naturales identificadas o identificables; es decir, allí se usa el término *información* para definir dato. También señala que datos sensibles o datos personales sensibles son los que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, el origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida

[1148] Guatemala, Corte de Constitucionalidad de Guatemala, *Expediente 1356-2006,* 2016, accedido 14 de mayo de 2017, http://www.oas.org/es/sla/ddi/docs/G5%20EXPEDIENTE%201356.2006.pdf.

sexual, situación moral y familiar u otras cuestiones íntimas de similar naturaleza. De esta forma, se supera la referencia implícita que realizaba la Constitución e incorpora un elemento fundamental en el contenido esencial del derecho que es la compresión adecuada de dato e información como garantía de su efectiva vigencia.

c) Sujeto activo

La norma constitucional que reconoce el derecho utiliza la frase genérica *toda persona* lo que incluye personas naturales y jurídicas, criterio que luego se desarrolla en la Ley de Acceso a la Información Pública. Sin embargo, aunque el Estado es una persona jurídica no existe constancia de este reconocimiento a su favor.

d) Sujeto pasivo

El artículo 35 de la Constitución de Guatemala señala solamente a los registros estatales como aquellos que pueden ser susceptibles de protección, de tal forma que el primer sujeto obligado es el Estado.

e) Objeto o bien jurídico

a. Derecho de información

De la lectura de la norma constitucional guatemalteca de 1985, artículo 3, consta expresamente el derecho de toda persona a conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica. Nuevamente, la dificultad de la norma se basa en la limitación a ficheros del Estado, ya que el derecho de información no solo se refiere al conocimiento de los datos registrados sino, incluso, de las finalidades para las cuales estos podrán ser usados.

b. Autodeterminación informativa

No consta ni en la Constitución ni en la normativa legal referencia a este contenido esencial propio del derecho a la protección de datos personales.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

La Ley de Acceso a la Información Pública, Decreto 57-2008, en el artículo 32[1149] establece varias excepciones al consentimiento. En realidad el legislador, mediante una

[1149] "Artículo 32. Excepción del consentimiento. No se requerirá el consentimiento del titular de la información para proporcionar los datos personales en los siguientes casos:
1. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;
2. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades del Estado, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;
3. Cuando exista una orden judicial;
4. Los establecidos en esta ley;
5. Los contenidos en los registros públicos;
6. En los demás casos que establezcan las leyes.
En ningún caso se podrán crear bancos de datos o archivos con datos sensibles o datos personales sensibles, salvo que sean utilizados para el servicio y atención propia de la institución". Véase Congreso

autorización que otorga la ley, realiza un ejercicio de ponderación de derechos y establece los casos en los que prima un derecho o interés superior que faculte a recopilar, tratar o difundir datos. Se resumen en causas estadísticas, científicas o de interés general, cuando se transmitan entre sujetos obligados en ejercicio de sus facultades contenidos en los registros públicos, tanto por orden judicial, así como establecidos en las leyes.

d. Principios

Respecto de los principios que son parte fundamental del derecho a la protección de datos personales, si bien la norma no hace mención de ellos ni siquiera de manera implícita, si se los puede encontrar en la Ley de Acceso a la Información Pública, en el artículo 30, cuando se determinan las obligaciones de los sujetos pasivos respecto del *habeas data*; estas son:

i. Deber de información

Limitado a capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos. Pero en el artículo 31 de la misma ley consta como obligación tomar el consentimiento para la difusión, distribución o comercialización de los datos, evitando incurrir en un vicio de la voluntad, por lo tanto aparece la obligación de explicarse claramente las consecuencias de sus actos. De esta forma, se entiende que existe un deber de información que garantice una voluntad libre de vicios.

ii. Pertinencia

La actualización aparece como derecho no como principio. En el Decreto 57-2008, Ley de Acceso a la Información Pública, en el artículo 30, numeral 2, se señala que los sujetos tendrán la responsabilidad de que los datos almacenados sean adecuados, pertinentes y no excesivos, en relación con los propósitos para los cuales se hayan obtenido.

iii. Calidad

La actualización aparece como derecho no como principio. En el Decreto 57-2008, Ley de Acceso a la Información Pública, en el artículo 1, numeral 2, se señala que el objeto de la ley es: "2. Garantizar a toda persona individual el derecho a conocer y proteger los datos personales de lo que de ella conste en archivos estatales, así como de las actualizaciones de los mismos". Asimismo, el artículo 7 sobre la actualización de información señala que: "Los sujetos obligados deberán actualizar su información en un plazo no mayor de treinta días, después de producirse un cambio". Por su parte, el artículo 30 sobre el *habeas data* determina que "Los sujetos obligados serán responsables de los datos personales" y, en relación con estos, deberán: "4. Procurar que los datos personales sean exactos y actualizados...".

iv. Finalidad

---

de la República de Guatemala, *Decreto 57-2008, 23/09/2008, Ley de Acceso a la Información Pública*, accedido 11 de mayo de 2017, http://www.oas.org/juridico/pdfs/mesicic4_gtm_acceso.pdf.

El artículo 30 numeral 3, del Decreto 57-2008, Ley de Acceso a la Información Pública hace mención a la obligación del sujeto de poner a disposición de la persona individual el documento en el que se establezcan los propósitos para su tratamiento, a partir del momento en el cual se recaben datos personales.

v. Seguridad

El artículo 30, numeral 5, del Decreto 57-2008, señala la responsabilidad de los sujetos obligados a implementar las medidas necesarias que garanticen la seguridad, y en su caso confidencia o reserva de los datos personales, y eviten su alteración, pérdida, transmisión y acceso no autorizado.

vi. Consentimiento

Se trata de un consentimiento expreso por el cual se autoriza exclusivamente la utilización de los datos con fines comerciales. Además, el artículo 31 menciona que se trata de un consentimiento expreso que debe registrarse por escrito y que faculta a difundir, distribuir o comercializar sus datos personales.[1150]

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

Tanto de la norma constitucional que configura el derecho a la protección de datos personales, como de la garantía legal denominada *habeas data*, se pueden colegir varios derechos que pueden ser ejercidos por los titulares del derecho a la protección de datos personales, los cuales se analiza a continuación:

a. Derecho de acceso

De la lectura de la norma constitucional se deduce que en Guatemala la protección de los datos personales tiene como derecho primigenio el acceso a conocer de la existencia y de la finalidad de todo dato personal que conste en archivos, fichas o cualquier otra forma de registros estatales.

Respecto del *habeas data*, contemplado como garantía en la Ley de Acceso a la Información pública, el derecho de acceso consta tanto en el artículo 1, como en el artículo 30, cuando señala que toda persona interesada, sin discriminación alguna, tendrá el derecho a conocer y proteger los datos personales de lo que de ella conste en archivos estatales; además, que los sujetos obligados serán responsables de adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso presentados por los titulares de los datos.

[1150] "Artículo 31. Consentimiento expreso. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones, salvo que hubiere mediado el consentimiento expreso por escrito de los individuos a que hiciere referencia la información. El Estado vigilará que en caso de que se otorgue el consentimiento expreso, no se incurra en ningún momento en vicio de la voluntad en perjuicio del gobernado, explicándole claramente las consecuencias de sus actos". Ibíd.

Asimismo, en el artículo 33 de la referida ley aparece que este acceso permite a los titulares de los datos personales o sus representantes legales solicitar no solo el acceso, sino que les sean entregados datos personales del solicitante en un formato comprensible o se les conteste por escrito que no los tienen.[1151]

b. Derecho de corrección o rectificación y actualización

De otro lado, el artículo 30 de la Ley de Acceso a la Información Pública señala que los sujetos obligados serán responsables de los datos personales y están obligados a corregirlos y a buscar su exactitud y actualización. Así, se puede colegir que la normativa consagra tanto el derecho de corrección o rectificación, usando ambos términos como sinónimos, como también el de actualización de datos personales. Con el contenido del artículo 34 de la misma ley, se verifica que al referirse al tratamiento de los datos personales se señala el derecho de los titulares de los datos a modificarlos cumpliendo varios requisitos.[1152] Asimismo, tanto el artículo 1, numeral 2, como el artículo 7 determinan el derecho del titular de conocer y proteger los datos personales que consten en archivos estatales, así como de las actualizaciones de los mismos; y a su vez de la obligación de los sujetos de actualizar su información en un plazo no mayor de treinta días, después de producirse un cambio. Por tanto, se puede verificar que no solo se concibe como un derecho exigible por el titular del dato, sino de un deber que debe ser cumplido por el sujeto obligado aun cuando no haya sido incoado; se trata entonces del acatamiento de uno de los principios concebidos como la calidad de datos.

c. Derecho de oposición, cancelación y derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

No aparece ni en la norma constitucional ni en la legal referencia alguna a estos derechos.

d. Derecho de consulta al registro general de protección de datos personales

En Guatemala al ser los obligados sujetos estatales se utilizan sistemas electrónicos cuya finalidad es dar respuesta a las peticiones. Estos sujetos deberán establecer vías de acceso a la información pública bajo responsabilidad de la autoridad máxima y garantizarán que la información publicada sea fidedigna y legítima. La información publicada en los sistemas de información electrónicos, entre otros, deberá coincidir exactamente con los sistemas de administración financiera, contable y de auditoría; además esta deberá ser

[1151] "Artículo 33.- Acceso a los datos personales. Sin perjuicio de lo que dispongan otras leyes, sólo los titulares de la información o sus representantes legales podrán solicitarla, previa acreditación, que se les proporcione los datos personales que estén contenidos en sus archivos o sistema de información. Esta Información debe ser entregada por el sujeto obligado, dentro de los diez días hábiles siguientes contados a partir de la presentación de la solicitud, en formato comprensible para el solicitante, o bien de la misma forma debe comunicarle por escrito que el sistema de datos personales no contiene los referidos al solicitante". Ibíd.

[1152] "Artículo 34.- Tratamiento de los datos personales. Los titulares o sus representantes legales podrán solicitar, previa acreditación, que modifiquen sus datos personales contenidos en cualquier sistema de información. Con tal propósito, el interesado debe entregar una solicitud de modificaciones, en la que señale el sistema de datos personales, indique las modificaciones que desea realizar y aporte la documentación que motive su petición. El sujeto obligado debe entregar al solicitante, en un plazo no mayor de treinta días hábiles desde la presentación de la solicitud, una resolución que haga constar las modificaciones o bien, le informe de manera fundamentada, las razones por las cuales no procedieron las mismas". Ibíd.

actualizada en los plazos establecidos en esta ley. Si bien estos registros hacen alusión a información pública, sin embargo, el Estado al contener datos personales debe también utilizar estos sistemas para responder en tiempo y debida forma también acciones de *habeas data*.

e. Derecho a indemnización por daños causados

Respecto de este derecho, se aclara que la Ley de Acceso a la Información Pública establece una serie de infracciones constantes en los artículos 62, 63, 64, 65, 66 y 67. Estas normas tipifican delitos y establecen sanciones penales, pero señalan que por los mismos actos pueden también propiciarse otro tipo de responsabilidades como las administrativas y civiles. En consecuencia, determinadas estas responsabilidades, procede solicitar indemnizaciones por los daños y perjuicios causados, como consta expresamente reconocido en las mencionadas normas.

g) Habeas data

a. Legitimados activos

Se desarrolla la norma constitucional que utiliza la frase genérica *toda persona*, cuando en el artículo 5 de la Ley de Acceso a la Información Pública se señala como sujetos activos titulares del derecho a la protección de datos personales en su contenido limitado a ficheros públicos: toda persona individual o jurídica, pública o privada.[1153]

b. Legitimados pasivos u obligados

El artículo 4 de la Ley de Acceso a la Información Pública establece tres tipos de obligados: el que almacena, el que custodia o protege lo depositado y el que administra.[1154]

Asimismo, el artículo 6 de la citada ley señala como sujeto obligado "a toda persona individual o jurídica, pública o privada, nacional o internacional de cualquier naturaleza, institución o entidad del Estado, organismo, órgano, entidad, dependencia, institución y cualquier otro que maneje, administre o ejecute recursos públicos, bienes del Estado, o actos de la administración pública en general, que está obligado a proporcionar la información pública que se le solicite"[1155].

[1153] "Artículo 5. Sujeto activo. Es toda persona individual o jurídica, pública o privada, que tiene derecho a solicitar, tener acceso y obtener la información pública que hubiere solicitado conforme lo establecido en esta ley". Ibíd.

[1154] "Artículo 4.- Ámbito de aplicación. Toda la información relacionada al derecho de acceso libre a la información contenida en registros, archivos, fichas, bancos, o cualquier otra forma de almacenamiento de información pública, en custodia, depósito o administración de los sujetos obligados, se regirá por lo que establece la Constitución Política de la República de Guatemala y la presente ley". Ibíd.

[1155] "Artículo 6. Sujetos obligados. Es toda persona individual o jurídica, pública o privada, nacional o internacional de cualquier naturaleza, institución o entidad del Estado, organismo, órgano, entidad, dependencia, institución y cualquier otro que maneje, administre o ejecute recursos públicos, bienes del Estado, o actos de la administración pública en general, que está obligado a proporcionar la información pública que se le solicite, dentro de los que se incluye el siguiente listado, que es enunciativo y no limitativo:

c. Derechos tutelados por el habeas data

Conforme el artículo 9 de la Ley de Acceso a la Información Pública, se protege el derecho a la protección de datos personales, ya que al definir al *habeas data* señala que es la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización.

d. Procedencia del habeas data

Como se trata de una acción directa, esto es que se ejerce frente al propio Estado, opera sin necesidad de acto negativo previo; es decir, no necesita negarse el acceso, ni la solicitud de actualización, rectificación eliminación o anulación de datos erróneos o que afecten sus derechos. Es más, conforme señala el artículo 33 de la Ley de Acceso a la Información Pública, el acceso a los datos personales procede siempre que sea solicitado por los titulares de la información o sus representantes legales previa acreditación de tal condición. Asimismo, el artículo 34 de la citada ley señala que en el caso de presentar el recurso de *habeas data* con la finalidad de modificar los datos registrados, este procede cuando es solicitado por los titulares o sus representantes legales, antes de la acreditación de esta condición; en el documento se deben indicar las modificaciones que desea realizar y aportar la documentación que motive su petición. En ambos casos, el Estado tiene plazos de respuesta entre 10 y 30 días, respectivamente, y es obligatorio para el Estado dar contestación expresa de una respuesta negativa de la cual existe un recurso de revisión contemplado en el artículo 35 del mismo cuerpo legal.

---

1. Organismo Ejecutivo, todas sus dependencias, entidades centralizadas, descentralizadas y autónomas; 2. Organismo Legislativo y todas las dependencias que lo integran; 3. Organismo Judicial y todas las dependencias que lo integran; 4. Todas las entidades centralizadas, descentralizadas y autónomas; 5. Corte de Constitucionalidad; 6. Tribunal Supremo Electoral; 7. Contraloría General de Cuentas; 8. Ministerio Público; 9. Procuraduría General de la Nación; 10. Procurador de los Derechos Humanos; 11. Instituto de la Defensa Pública Penal; 12. Instituto Nacional de Ciencias Forenses de Guatemala; 13. Registro Nacional de las Personas; 14. Instituto de Fomento Municipal; 15. Instituto Guatemalteco de Seguridad Social; 16. Instituto de Previsión Militar; 17. Gobernaciones Departamentales; 18. Municipalidades; 19. Consejos de Desarrollo Urbano y Rural; 20. Banco de Guatemala; 21. Junta Monetaria; 22. Superintendencia de Bancos; 23. Confederación Deportiva Autónoma de Guatemala, federaciones y asociaciones deportivas nacionales y departamentales que la integran; 24. Comité Olímpico Guatemalteco; 25. Universidad de San Carlos de Guatemala; 26. Superintendencia de Administración Tributaria; 27. Superintendencia de Telecomunicaciones; 28. Empresas del Estado y las entidades privadas que ejerzan funciones públicas; 29. Organizaciones No Gubernamentales, fundaciones y asociaciones que reciban, administren o ejecuten fondos públicos; 30. Todas las entidades de cualquier naturaleza que tengan como fuente de ingresos, ya sea total o parcialmente, recursos, subsidios o aportes del Estado; 31. Las empresas privadas a quienes se les haya otorgado mediante permiso, licencia, concesión o cualquier otra forma contractual la explotación de un bien del Estado; 32. Organismos y entidades públicas o privadas internacionales que reciban, manejen o administren fondos o recursos públicos; 33. Los fideicomisarios y fideicomitentes de los fideicomisos que se constituyan o administren con fondos públicos o provenientes de préstamos, convenios o tratados internacionales suscritos por la República de Guatemala; 34. Las personas individuales o jurídicas de cualquier naturaleza que reciban, manejen o administren fondos o recursos públicos por cualquier concepto, incluyendo los denominados fondos privativos o similares; 35. Comités, patronatos, asociaciones autorizadas por la ley para la recaudación y manejo de fondos para fines públicos y de beneficio social, que perciban aportes o donaciones del Estado.
En los casos en que leyes específicas regulen o establezcan reservas o garantías de confidencialidad deberán observarse las mismas para la aplicación de la presente ley". Ibíd.

e. Procedimiento del habeas data

La garantía se efectúa de forma directa entre el sujeto activo y el sujeto obligado. Dicho de otro modo, es el Estado el que debe realizar la entrega de información, las correcciones, rectificaciones y actualizaciones. Únicamente, si existe una negativa por parte del obligado podrá interponerse un recurso de revisión de conformidad con lo señalado en el artículo 35 de la misma ley.

h) Institucionalidad de protección

Respecto de la autoridad que debe vigilar y proteger los datos personales, el artículo 46 de la ley en mención señala que el encargado[1156] es el Procurador de los Derechos Humanos.[1157]

i) Régimen sancionador

El Código Penal de Guatemala, que ha sufrido varias reformas desde su versión original, incluyó en el año 2009 una modificación al artículo 190[1158] incorporando el delito de violación a la intimidad sexual. En el artículo 274 D[1159] se sanciona la creación de bases de datos que pueda afectar la intimidad y el artículo 274 F tipifica la utilización sin autorización de registros informáticos de otros.[1160]

[1156] "ARTICULO 46. Autoridad reguladora. El acceso a la información pública como derecho humano fundamental previsto en la Constitución Política de la República de Guatemala y los tratados o convenios internacionales en esta materia ratificados por el Estado de Guatemala, estará protegido por el Procurador de los Derechos Humanos en los términos de la Ley de la Comisión de los Derechos Humanos del Congreso de la República y del Procurador de los Derechos Humanos, Decreto Número 54-86 del Congreso de la República". Ibíd.

[1157] Guatemala, *Procurador de los Derechos Humanos*, accedido 2 de octubre de 2017, https://www.pdh.org.gt/biblioteca/documentos.html.

[1158] "ARTICULO 190.* Violación a la intimidad sexual. Quien por cualquier medio sin el consentimiento de la persona, atentare contra su intimidad sexual y se apodere o capte mensajes, conversaciones, comunicaciones, sonidos, imágenes en general o imágenes de su cuerpo, para afectar su dignidad, será sancionado con prisión de uno a tres años.

Las mismas penas se impondrán al que, sin estar autorizado, se apodere, acceda, utilice o modifique, en perjuicio de tercero, comunicaciones efectuadas por cualquier medio físico o electrónico o datos reservados con contenido sexual de carácter personal, familiar o de otro, que se encuentren registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo o registro público o privado, en perjuicio de la persona titular de los datos o de una tercera persona.

Se impondrá prisión de dos a cuatro años a quien difunda, revele o ceda, a cualquier título, a terceros, los datos o hechos descubiertos o las imágenes captadas a que se refiere este artículo. *Reformado por el Artículo 34, del Decreto Del Congreso Número 9-2009 el 03-04-2009". Guatemala, *Decreto No. 17-73 Código Penal*, 1973, accedido 14 de mayo de 2017, https://www.oas.org/dsp/documents/trata/Guatemala/Legislacion%20Nacional/Codigo%20Penal%20Guatemalteco%20DECRETO%20DEL%20CONGRESO%2017-73.doc.

[1159] "ARTICULO 274.- * "D". Registros prohibidos. Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas. *Adicionado por el artículo 16, del *Decreto Número 33-96 del Congreso de la República de Guatemala*. Ibíd.

[1160] "ARTICULO 274.- * "F". Uso de información. Se impondrá prisión de seis meses a dos años, y multa de doscientos a mil quetzales al que, sin autorización, utilizare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos. *Adicionado por el Artículo 18, del Decreto Número 33-96 Del Congreso de la República de Guatemala". Ibíd.

La Ley de Acceso a la Información Pública reconoce la existencia de infracciones penales como la referencia expresa que consta en el artículos 37[1161] con relación a la información, documentos y expedientes que formen parte de los archivos administrativos que no podrán, en ningún caso, ser destruidos, alterados o modificados sin justificación. Además de la mencionada norma, existen otras como los artículos 62, 63, 64, 65, 66 y 67 que establecen responsabilidades administrativas. Finalmente, en las normas señaladas también se hace alusión a responsabilidades civiles con indemnizaciones por los daños y perjuicios causados.

j) Transferencia internacional de datos

No existe norma constitucional o legal que haga alusión al tema de transferencia internacional de datos de carácter personal.

2.2 Brasil (1988)

En la Constitución Política de la República Federativa de Brasil de 1988, en el artículo 5, relativo a los derechos garantizados a los brasileños y a los extranjeros residentes en el país, se reconoce como inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurándose el derecho a indemnización por el daño material o moral derivado de su violación.

Respecto del derecho a la protección de datos personales, Brasil se apartó de la tendencia instaurada por:

> [...] las constituciones de Portugal y España— de establecer únicamente un derecho de control sobre los datos de carácter personal o de pregonar que la informática no debe afectar a la intimidad de las personas —aunque sin establecer los principios relativos al tratamiento de los datos ni reconocer expresamente un derecho al control de los mismos—, reconocerá por primera vez una garantía específica del derecho a la protección de los datos, bautizándola «hábeas data», en clara simetría con la acción de hábeas corpus —como se observará sólo a estas dos acciones se las reconoce como «gratuitas». Como se habrá observado, la Constitución brasileña no trazó un dispositivo autónomo que contemplara el derecho de conocer y de rectificar datos de carácter personal, sino que ese derecho fue otorgado en el mismo dispositivo que instituye el remedio de su tutela.[1162]

[1161] "Artículo 37. Archivos administrativos. Con relación a la información, documentos y expedientes que formen parte de los archivos administrativos no podrán en ningún caso ser destruidos, alterados o modificados sin justificación. Los servidores públicos que incumplan el presente y el anterior artículo de esta ley podrán ser destituidos de su cargo y sujetos a lo previsto por los artículos 418 Abuso de Autoridad y 419 Incumplimiento de Deberes del Código Penal vigente. Si se trata de particulares quienes coadyuven, provoquen o inciten, directa o indirectamente a la destrucción, alteración o modificación de archivos históricos, aplicará el delito de depredación del patrimonio nacional, regulado en el Código Penal". Guatemala, Congreso de la República de Guatemala, *Decreto 57-2008, 23/09/2008, Ley de Acceso a la Información Pública*, ibíd.

[1162] J. A. DA SILVA, *Curso de direito constitucional positivo* (San Pablo, Malheiros, 1992), 397.

La Constitución brasileña reconoce la institución del *habeas data* conceptualizada como un derecho sustantivo de acceso a información de carácter personal, y a la vez como una garantía jurisdiccional para una tutela constitucional efectiva.

Es fundamental señalar que esta tendencia procesal constitucional nace de una realidad propia de los pueblos latinoamericanos ya que:

> [...] el hábeas data fue incorporado a la Constitución brasileña de 1988, como consecuencia de la proyección de las disposiciones sobre protección de datos de carácter personal contenidas en la Constitución de Portugal de 1976, las cuales fueron establecidas, en gran medida, con el fin de permitir el acceso a las informaciones que se encontraban en poder de la arbitraria y violenta policía política, creada por Oliveira Salazar. De manera similar, en el Brasil, la Policía y el Servicio Nacional de Informaciones se ocupaban de determinar quiénes eran los opositores al régimen de facto que culminó en 1985, y de perseguirlos. Por ello, con la misma finalidad que motivó la incorporación de la norma portuguesa, y en la inteligencia de facilitar el ingreso a tales archivos y permitir actuar sobre ellos, se consagró el hábeas data. Sin embargo, los fines originariamente buscados con este nuevo instituto encontraron ciertos escollos a la hora de la aplicación efectiva, en particular, por la creencia acerca de que el Estado debe tener secretos, lo cual es un vicio tradicional que viene del pasado colonial, mantenido incluso hasta mucho tiempo después de la independencia latinoamericana, por efecto del régimen de monarquía constitucional.[1163]

Tal y como sus predecesoras, la norma constitucional consagra el derecho de los particulares de conocer los datos que el Estado guarda en las bases de datos o ficheros administrados por él.

El artículo 5 de la Constitución de la República Federativa de Brasil de 1988 expresamente señala:

> Todos son iguales ante la ley, sin distinción de cualquier naturaleza, garantizándose a los brasileños y a los extranjeros residentes en el País la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la prioridad, en los siguientes términos: LXXII Se concederá hábeas data: a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo; [...] LXXVII son gratuitas las acciones de "hábeas corpus" y "hábeas data" y, en la forma de la ley, los actos necesarios al ejercicio de la ciudadanía.[1164]

Ahora bien, las normas vigentes son:

a) La Ley 12.965, 23 de abril de 2014, establece los principios, garantías, derechos y deberes para el uso de internet en Brasil, denominado Marco Civil Brasileño de Internet, que consagra el derecho a la protección de datos personales.

[1163] D. DE ABREU DALLARI, (disertación, Seminario Iberoamericano sobre acción de *hábeas data*, Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, Chile, 9 a 11 de abril de 1997), citado por O. PUCCINELLI, *Tipos y subtipos*, accedido 8 de junio de 2007, http://www.infobaeprofesional.com/adjuntos/documentos/08/0000887.pdf.

[1164] Brasil, *Constitución Política de 1988*, accedido 22 de mayo de 2017, http://pdba.georgetown.edu/Constitutions/Brazil/esp88.html.

> Artículo 7.- El acceso a Internet es esencial para el ejercicio de la ciudadanía y para los usuarios están garantizados los siguientes derechos: [...] VIII – información clara y completa sobre la recogida, uso, almacenamiento, tratamiento y protección de sus datos personales, que sólo podrán ser utilizados para finalidades que: a) justifiquen su recolección; b) no estén prohibidas por ley; y c) queden especificadas en los contratos de prestación de servicios o en los términos de uso de las aplicaciones de Internet.[1165]

Los otros derechos reconocidos en el Marco Civil Brasileño de Internet constan descritos en el artículo 3 de la ley citada, por el cual se determina que la disciplina de la utilización de Internet en Brasil cuenta con principios entre los que constan: la garantía de la libertad de expresión, la comunicación y la manifestación del pensamiento, según la Constitución Federal; la protección de la privacidad; y protección de los datos personales, en forma de la ley. Asimismo, el artículo 10 de la norma citada señala que la custodia y entrega de los registros de conexión y de acceso a aplicaciones de Internet de que trata esta ley, así como de los datos personales y del contenido de las comunicaciones privadas, deben atender a la preservación de la intimidad, de la vida privada, de la honra y de la imagen de las partes directa o indirectamente involucradas.

b) Decreto 8.771, de 11 de mayo de 2016, que "*Regulamenta a Lei no* 12.965, de 23 de abril de 2014, *para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações*"[1166], de ahora en adelante reglamento al Marco Civil brasileño.

Sobre normativa sectorial que regula la protección de datos personales consta en la Ley 9.507 de 1997; por su parte el Acceso a la Información que determina el manejo de información personal en ficheros públicos en aplicación del derecho se contiene en el artículo 5 XXXII de la Constitución de la República Federativa de Brasil de 1998 que dice:

> Artículo 5.- Todos son iguales ante la ley, sin distinción de cualquier naturaliza, garantizándose a los brasileños y a los extranjeros residentes en el País la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la prioridad, en los siguientes términos: XXXII. relativo todos tienen derecho a recibir de los órganos públicos informaciones de su interés particular, o de interés colectivo o general, que serán facilitados en el plazo señalado en la ley, bajo pena de responsabilidad, salvo aquellas cuyo secreto sea imprescindible para la seguridad de la sociedad y del Estado.

Existe además, la Ley 9.296 de 1996, sobre la intercepción de comunicaciones telefónicas; Ley 10.406, de 10 de enero de 2002; el Código Civil que alude a la inviolabilidad de la vida privada; y el Código Penal que tipifica diversos delitos relacionados con la privacidad.

Para el 14 de agosto de 2018, el Congreso Nacional aprobó un marco legal para el tratamiento y uso de datos personales denominado, Ley de Protección de Datos

[1165] "Marco Civil Brasileño de Internet en Español, *Ley 12.965*, de 23 de abril de 2014, que establece los principios, garantías, derechos y deberes para el uso de Internet en Brasil".
[1166] Brasil, Presidencia de la República Federativa del Brasil, *Decreto n.º 8771*, Regulamenta a Lei no 12.965, de 23 de abril de 2014.

Personales, LGPD, 13,709/18[1167]. Cuyo objetivo es proteger a los titulares de los datos en su derecho fundamental, promover la innovación y el desarrollo económico y tecnológico. Este "texto final concilia la protección de garantías y libertades fundamentales con los intereses económicos"[1168]. Fue aprobada por unanimidad en la Cámara y en el Senado y su ámbito de aplicación incluye los sectores público y privado. Sin embargo, pese a su promulgación esta normativa fue vetada en lo relativo a la institucionalidad.

El 28 de diciembre de 2018, Michael Temer, dicta una Orden Ejecutiva denominada Medida Provisoria No. 869/18[1169] por la que crea la Autoridad Nacional Brasileña de Protección de Datos, ANPD, institución "dependiente de la Presidencia de la República. En el necesario paso por el Congreso para transformar la medida en ley, se determinó que la autoridad sería sometida a revisión dos años después de entrar en operaciones. Así, bajo este escenario, la solución de cualquier controversia u omisión quedará a cargo de un ente administrativo carente de recursos e independencia política del gobierno de turno"[1170].

Posteriormente, la Cámara de Diputados de Brasil aprobó el 28 de mayo la Medida Provisional 869/18. El martes 9 de julio de 2019, en Boletín Oficial Federal se publicó la Ley 13.853/19[1171] que tiene su origen dicha Medida Provisional y que modifica la Ley LGPD, 13,709/18, para establecer la protección de datos personales y crear la Autoridad Nacional de Protección de Datos; y hace otros arreglos y que es sancionada por el presidente Jair Bolsonaro con nueve vetos.

A continuación se examinarán aquellos elementos que nos permitirán construir un contenido esencial del derecho a la protección de datos personales en Brasil. El análisis se hará respecto de la normativa vigente, integrando los textos constitucionales y legales de carácter general vigentes a la fecha:

a) Ámbito: Registros o ficheros públicos y privados

El artículo 5 de la Constitución de la República Federativa del Brasil de 1988 expresamente señala que el único ámbito aplicable es el de los ficheros públicos cuando manifiesta de forma expresa: "LXXII Se concederá hábeas data: a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público..."[1172].

[1167] Brasil, Ley N ° 13.709, de 14 de agosto de 2018, accedido el 20 de agosto de 2018, http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

[1168] Coalizão Direitos na Rede "Temer: sancione sin cambios la ley de Protección de Datos en Brasil", Asociación para el Progreso de las Comunicaciones, accedido 19 de agosto de 2019 https://www.apc.org/es/pubs/temer-sancione-sin-cambios-la-ley-de-protecci%C3%B3n-de-datos-en-brasil

[1169] Brasil, Medida Provisional 869/18, accedido el 20 de agosto de 2019, http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/57220361/do1-2018-12-28-medida-provisoria-n-869-de-27-de-dezembro-de-2018-57219992

[1170] J. VENTURINI, "¿Bajo qué términos se protegerán los datos en Brasil?", @derechosdigitales, accedido 19 de agosto de 2019 https://www.derechosdigitales.org/13499/bajo-que-terminos-se-protegeran-los-datos-en-brasil/

[1171] Brasil, Ley N ° 13.853 del 8 de julio de 2019, accedido el 20 de agosto de 2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1

[1172] Brasil, *Constitución de 1988*, accedido 22 de mayo de 2017, http://pdba.georgetown.edu/Constitutions/Brazil/esp88.html.

Esta norma constitucional no ha sido modificada, por lo que respecto del *habeas data* este tiene un ámbito limitado.

Ahora bien, el Marco Civil Brasileño de Internet, promulgado en el 2014, consagra a favor de las personas naturales el ejercicio del derecho a la protección de datos personales, conforme consta en el artículo 7 VIII antes citado, pues faculta a las personas a solicitar información sobre la recogida, uso, almacenamiento, tratamiento y protección de sus datos personales. El artículo 9º del mismo texto legal, al referirse a la neutralidad de la red, señala la obligación de los responsables de transmisión, conmutación o ruteo de tratar de forma igual cualquier paquete de datos, sin distinción por contenido, origen y destino, servicio, terminal o aplicación; se colige que el ámbito de aplicación ya no se limita al ámbito público, sino que este derecho también puede ser efectivizado en el ámbito privado.

Además, el Marco Civil Brasileño es norma que regula los derechos y garantías de los usuarios, la provisión de conexión y de aplicaciones de internet, la neutralidad de la red, la protección a los registros, datos personales y comunicaciones privadas, la custodia de registros de conexión, de acceso a aplicaciones de internet en la provisión de conexión y de aplicaciones, la responsabilidad por daños que surgieran del contenido generado por terceros, la solicitud judicial de registros y el ejercicio del Poder Público. Así, se puede verificar que la citada ley es aplicable, tanto al ámbito público como al privado y en consecuencia en Brasil, a partir de la vigencia de esta norma, los datos personales se protegen tanto en ficheros públicos como privados.

Finalmente, conforme el artículo 1 de la Ley LGPD, 13,709/18 con vetos en adelante, LGPD el objetivo de esta norma prevé el procesamiento de datos personales en medios físicos y digitales, por parte de una persona jurídica y natural regida por el derecho público o privado.

En el mismo sentido, lo señalado por el artículo 3 de la LGPD que determina que el ámbito de aplicación de esta ley es cualquier operación de tratamiento realizada por persona natural o por persona jurídica de derecho público o privado, independientemente del medio, del país de su sede o del país donde estén localizados los datos , siempre y cuando se cumplan una serie de condiciones.[1173]

b) Naturaleza del dato

En la Constitución de la República Federativa del Brasil de 1988, en el artículo 5, respecto de la procedencia del *habeas data* expresamente se señala que será aplicable para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público,[1174] coligiéndose que el presupuesto de protección es la información personal, la

[1173] Que "I- la operación de tratamiento se lleva a cabo en el territorio nacional; II - la actividad de procesamiento tiene el propósito de ofrecer o suministrar bienes o servicios o el procesamiento de datos de individuos ubicados en el territorio nacional; o III - los datos personales objeto del procesamiento se han recopilado en el territorio nacional. Párrafo 1. Los datos personales cuyo titular se encuentre allí en el momento de la recopilación se considerarán recopilados en el territorio nacional. Párrafo 2 Las disposiciones del artículo I de este artículo no están sujetas al procesamiento de los datos previstos en el artículo IV de la sección de art. 4 de esta Ley", artículo 3 de la LGPD.
[1174] Ibíd.

cual puede constar en registros o bancos de datos; de tal forma que no se hace mención a si el soporte debe ser físico o virtual ni a su automatización, sino a que se encuentre registrado o almacenado junto a otros datos.

La Ley 12.527, 18 de noviembre de 2011, denominada Ley General de Acceso a la Información Pública, señala el concepto de información personal en el artículo 4, IV determinando que es aquella relacionada con la persona natural identificada o identificable. Lamentablemente, la esfera de aplicación de esta norma se limita a ficheros públicos.

Posteriormente, con la Ley 12.965, 23 de abril de 2014, en adelante el Marco Civil Brasileño de Internet no hace mención al concepto del presupuesto del derecho a la protección de datos personales, esto es a la información o datos de carácter personal. Sin embargo, el reglamento al Marco Civil Brasileño aclara perfectamente este tema, ya que en el artículo 14 explica que el concepto de dato personal es aquel relacionado a la persona natural identificada o identificable, incluyendo números identificativos, datos locacionales o identificadores electrónicos siempre que estos estén relacionados con una persona.[1175] De esta manera este concepto se adecua a los términos generales utilizados en la normativa europea.

El Reglamento al Marco Civil de Internet en el artículo 10 § 3º, señala respecto a la atención de la preservación de la intimidad, vida privada, honra e imagen, que esto no impide a las autoridades administrativas que detenten competencia legal para hacerlo, el solicitar datos de registro que contengan información personal, filiación y dirección, de conformidad también con el artículo de la Ley de Marco Civil de Internet. Estos datos se denominan datos catastrales y son aquellos referentes a la filiación, la dirección y los de calificación personal, entendida como nombre, prenombre, estado civil y profesión del usuario (art. 11 § 2º de la citada ley). De esta forma existe una categoría propia de la legislación brasileña denominada dato catastral que es aquel grupo de datos que el Estado está autorizado por ley a recabar de sus ciudadanos.

Respecto del formato en el que se deben almacenar los datos, queda claro que se refiere a datos digitales toda vez que, conforme señala el artículo 15 del citado reglamento, los datos deberán almacenarse y mantenerse en formato interoperable y estructurado, para facilitar el acceso resultante de decisión judicial o determinación legal, respetando las directrices sobre estándares de seguridad enumeradas en el artículo 13 de este Decreto.[1176]

Conforme el artículo 1 de la LGPD, los datos personales, que son objeto de esta Ley, podrán estar en soporte físico o digital. Por su parte, el artículo 3 de la LGPD determina que en el ámbito de la ley se encuentran los citados datos, independientemente del medio de soporte. Finalmente, el artículo 5 de la LGPD al definir a una base de datos

[1175] "Artículo 14. Para os fins do disposto neste Decreto, considerase: I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa...". Brasil, Presidencia de la República Federativa del Brasil, *Decreto nº 8771*, Regulamenta a Lei no 12.965, de 23 de abril de 2014.

[1176] "Artículo 15. Os dados de que trata o art. 11 da Lei 12.965, de 2014, deverão ser mantidos em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal, respeitadas as diretrizes elencadas no art. 13 deste Decreto", ibíd.

señala que “son el conjunto estructurado de datos personales, establecido en uno o en varios lugares, en soporte electrónico o físico”.

El citado artículo 5 de la LGPD señala que dato personal es “aquella información relacionada con la persona natural identificada o identificable”. De esta forma la normativa adopta el estándar internacional de protección.

En cuanto a dato sensible, el citado artículo 5, señala que es “aquel relativo al origen racial o étnico, convicción religiosa, opinión política, afiliación a sindicato o la organización de carácter religioso, filosófico o político, dado referente a la salud o a la vida sexual, dato genético o biométrico, cuando está vinculado a una persona natural”. En este concepto podemos destacar positivamente el uso de terminología precisa, esto es la utilización de la frase *opinión política* en lugar de la ambigua palabra *ideología*. De otro lado, se zanja discusiones previstas en otras normativas y se incluye a los datos genéticos y biométricos como datos sensibles.

Además, el artículo 11 de la LGPD estipula que el tratamiento de datos personales sensibles procederá únicamente si el titular ha consentido en ello. Pero además, establece una lista taxativa de casos en los que procede el tratamiento de este tipo de datos personales sin autorización del titular y se refieren a: el cumplimiento de una obligación legal privada o pública; la realización de estudios de investigación; el ejercicio de derechos contractuales y judiciales; la protección de la vida o de la salud; la prevención del fraude y la seguridad del titular.

Sobre dato anonimizado, el artículo 5 de la LGPD determina que es aquel que “no puede ser identificado utilizando medios técnicos razonables y disponibles en el momento de su tratamiento”. Pero además se establece el concepto de anonimización, es decir la utilización de medios técnicos razonables y disponibles que impidan la asociación, directa o indirecta del dato a un individuo. Finalmente, el artículo 12 aclara que el proceso de anonimización puede ser revertido y que de ocurrir este supuesto se considerará dato personal.

Respecto de datos de salud, el artículo 13 de la LGPD, determina que estos podrán ser tratados únicamente para estudios de investigación realizados exclusivamente dentro del órgano y mantenidos en un ambiente controlado y seguro.

c) Sujeto activo

Respecto del derecho a la protección de datos que aparece consagrado en el artículo 7º VIII del Marco Civil Brasileño, se colige que son todas las personas, que a efectos de la ley se denominan ciudadanos o usuarios. Estos términos no hacen alusión a persona jurídica, pues por su contenido se refieren exclusivamente a personas naturales que son las únicas que pueden ejercer derechos políticos o relacionarse en una posición de consumo respecto de un proveedor de bienes y servicios. En consecuencia, este derecho tendría como sujeto activo exclusivamente a la persona natural.

Asimismo, la Constitución brasileña, desde la postura dualista que señala que cuando se consagra una garantía o mecanismo constitucional se reconoce además un derecho fundamental, podemos concluir que el titular del *habeas data*, lo sería también del derecho a la protección de datos personales. En consecuencia, serán sujeto activo las

personas naturales brasileñas y extranjeras residentes en el país, de conformidad con lo señalado en el artículo 5 de la Constitución brasileña.[1177]

Ahora bien, el § 3º del artículo 10 del Marco Civil de Internet señala que pueden solicitar acceso a datos personales de los ciudadanos relativos a la calificación personal, entendida como nombre, prenombre, estado civil y profesión del usuario,[1178] la filiación y la dirección, las autoridades administrativas que detenten competencia legal para su solicitud, de acuerdo con la ley. Norma que se desarrolla en los artículos 11 y 12 del Reglamento en mención, pues determina los requisitos de la solicitud.

Por su parte, el artículo 5 de la LGPD en el glosario de términos define al titular como la persona natural a que refieren los datos personales objeto de tratamiento. De esta manera se cierra la problemática de determinar si este derecho es prerrogativa de las personas jurídicas, pues de la clara lectura del texto se colige que este derecho es exclusivo de las personas naturales.

Finalmente, la sección III sobre procesamiento de datos personales niños y adolescentes como titulares de derechos, en su artículo 14 señala que solo podrán tratarse en su mejor interés, con el consentimiento específico y destacado dado por al menos uno de los padres o el responsable legal, a menos que la recolección sea necesaria para contactar a los padres o al responsable legal, siempre que los datos personales se utilicen por única vez y sin almacenamiento, o para su protección. Se establece al responsable la obligación adicional de mantener pública la información sobre los tipos de datos recolectados, la forma de su utilización y los procedimientos para el ejercicio de los derechos.

d) Sujeto pasivo

Como se mencionó en el citado artículo 9º del Marco Civil de Internet, al referirse a la neutralidad de la red, consta como sujeto pasivo el responsable de transmisión, conmutación o ruteo, obligado a tratar de forma igual cualquier paquete de datos, sin distinción por contenido, origen y destino, servicio, terminal o aplicación.

Ahora bien, conforme consta en el artículo 10 del Marco Civil de Internet brasileño, el proveedor responsable de la custodia y entrega de los registros de conexión y de acceso a aplicaciones de Internet de que trata esta ley, así como de los datos personales y del contenido de las comunicaciones privadas, será obligado a entregar los mencionados registros de forma autónoma o asociados a datos personales u otras informaciones que

[1177] Brasil, *Constitución de 1988*, accedido 22 de mayo de 2017, http://pdba.georgetown.edu/Constitutions/Brazil/esp88.html.

[1178] "Art. 11. Las autoridades administrativas a que se refiere el art. 10, § 3º de la Ley Nº 12.965, de 2014, indicarán el fundamento legal de competencia expresa para el acceso y la motivación para la solicitud de acceso a los datos catastrales. § 1º El proveedor que no recolecta datos catastrales deberá informar a la autoridad solicitante de la misma, quedando excluido de proporcionar dichos datos. § 2º Se consideran datos catastrales: l) I - la filiación; m) II - la dirección; Y de los demás. n) III - la calificación personal, entendida como nombre, prenombre, estado civil y profesión del usuario. o) § 3º Las solicitudes de que trata el capítulo deben especificar a los individuos cuyos datos están siendo requeridos y la información deseada, siendo vedadas solicitudes colectivas que sean genéricas o inespecíficas". Brasil, Presidencia de la República Federativa del Brasil, *Decreto nº 8771, Regulamenta a Lei no 12.965*, de 23 de abril de 2014.

puedan contribuir a la identificación del usuario o del terminal, únicamente mediante orden judicial, tal como queda dispuesto en la Sección IV de la norma citada.

De la comprensión de estas normas se colige que serán sujetos pasivos del derecho a la protección de datos personales el proveedor responsable de la custodia, transmisión, conmutación o ruteo y entrega de los registros de conexión y de acceso a aplicaciones de Internet, así como de los datos personales y de contenido de las comunicaciones privadas. En este caso estos proveedores pueden ser personas naturales o jurídicas que en una relación de consumo toman el lugar de contraparte del usuario.

Por su parte, el artículo 5 de la LGPD establece en el listado de términos al controlador, quien será "la persona natural o jurídica, de derecho público o privado, a quien le competen las decisiones referentes al tratamiento de datos personales". Que además, en virtud del artículo 37 de la LGPD, deberá mantener "registro de las operaciones de tratamiento de datos personales que realicen, especialmente cuando se base en el legítimo interés". Así como, indicar la identidad y las informaciones de contacto del encargado "de forma clara y objetiva, preferentemente en el sitio electrónico del controlador", conforme señala el artículo 41 de la LGPD. Finalmente, el controlador está en la obligación de verificar el cumplimiento de las propias instrucciones y de las normas sobre la materia, conforme señala el artículo 39 de la LGPD. Entonces, el término controlador coincide con el de responsable de tratamiento, de esta forma se alinea al estándar internacional.

En el citado artículo 5 de la LGPD consta el término operador que coincide con el concepto de encargado establecido en el estándar internacional, ya que lo considera como la persona natural o jurídica, de derecho público o privado, que realiza el tratamiento de datos personales en nombre del controlador.

Se aclara que se consideran agentes de tratamiento tanto al controlador como al operador conforme el numeral IX del artículo 5 de la LGPD, de esta forma se deja claro que los dos sujetos pasivos pueden tener responsabilidad en el tratamiento inadecuado de datos personales.

Finalmente, el numeral VIII del artículo 5 de la LGPD establece el concepto de responsable como aquella persona natural, indicada por el controlador, que actúa como canal de comunicación entre el controlador, los titulares y la Autoridad Nacional de Protección de Datos (ANPD). Esta definición corresponde al delegado de protección de datos que está reconocido en la normativa europea, por lo que de esta manera la normativa brasileña se aliena al mayor estándar de protección vigente.

e) Objeto o bien jurídico

La LGPD establece en el artículo 17 que "toda persona natural tiene asegurada la titularidad de sus datos personales y garantizados los derechos fundamentales de libertad, de intimidad y de privacidad, en los términos de esta Ley". De esta manera se coloca a la persona y por ende a su manifestación básica, el dato, como centro de protección en los entornos digitales. Del reconocimiento de los derechos a la protección de datos personales, a través de la autodeterminación informativa cuando se señala que se garantiza su titularidad, y la de otros derechos fundamentales como la libertad, la

intimidad y la privacidad, se determina la autonomía de cada uno de los derechos que están en juego en la interrelación personal y tecnologías de la información y comunicación. Es objetivo fundamental de esta normativa la protección integral del individuo en espacios digitales porque al reconocer estos derechos se protege su dignidad.

a. Derecho de información

El artículo 7.º VIII del Marco Civil de Internet brasileño, al determinar el derecho a la protección de datos personales, señala expresamente que las personas tienen derecho a información clara y completa sobre la recogida, uso, almacenamiento, tratamiento y protección de sus datos personales. Es decir, el derecho de información permite al titular de los datos conocer cada una de las fases del procesamiento de datos.

Por su parte el artículo 5 de la Constitución brasileña señala que se *concederá hábeas data para para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público*.[1179] Es decir, las personas podrán ejercer su derecho de información utilizando esta garantía constitucional.

El artículo 9 de la LGPD determina que "el titular tiene derecho a un fácil acceso a la información sobre el procesamiento de sus datos, que debe estar disponible de manera clara, apropiada y abierta" anotándose que al menos debe ser de libre acceso lo siguiente: el propósito específico del tratamiento; la forma y duración del tratamiento; la identificación del controlador y su información de contacto; el uso compartido de datos por el controlador y el propósito; responsabilidades de los agentes que realizarán el tratamiento; y derechos del titular. Pero además, se añade que de no cumplirse con el deber de información por parte del responsable, el consentimiento se considerará nulo y sin efecto, conforme reza el Párrafo 1 del citado artículo. De producirse cambios incompatibles en el propósito original del procesamiento de datos personales, el controlador informará al titular por adelantado de los cambios a fin de que este pueda revocar el consentimiento si no está de acuerdo, conforme señala el Párrafo 2 de la misma norma. Finalmente, el titular tiene derecho a conocer si sus datos serán procesados para la provisión de un producto o servicio así como a conocer sobre los medios por los cuales puede ejercer sus derechos, al tenor del Párrafo 3.

Por su parte, el artículo 18 de la LGPD establece que:

> […] el titular de los datos personales tiene derecho a obtener del controlador, en relación con los datos del titular por él tratados, en cualquier momento y mediante solicitud: […] VII - información de las entidades públicas y privadas con las cuales el controlador realizó uso compartido de datos; VIII - información sobre la posibilidad de no proporcionar consentimiento y sobre las consecuencias de la negativa […]

El derecho de información se encuentra evidenciado en el principio de transparencia recogido en el artículo 6 de la LGPD, en el citado artículo 9 de la LGPD, así como en el artículo 18 de la LGPD, destacándose su adaptación al RGDP, ya que en estas normas se realiza el listado de contenidos mínimos a ser informados; se menciona expresamente

[1179] Brasil, *Constitución de 1988*, accedido 22 de mayo de 2017, http://pdba.georgetown.edu/Constitutions/Brazil/esp88.html.

el deber de información sobre los cambios en la finalidad y por tanto, en el procesamiento, para que el titular pueda, de ser el caso, revocar su consentimiento; la posibilidad de no proporcionar los datos y las consecuencias de la no entrega. Estos elementos son parte del estándar europeo. Finalmente, una precisión propia de la normativa brasileña que obliga a informar sobre las entidades públicas y privadas con las cuales el controlador realizó uso compartido de datos.

b. Autodeterminación informativa

El artículo 7 VII del Marco Civil de Internet brasileño señala la prohibición y por tanto, la imposibilidad de suministrar a terceros sus datos personales, incluyendo registros de conexión y de acceso a aplicaciones en Internet, salvo mediante consentimiento libre, expreso e informado o en circunstancias establecidas por la ley.

Esta norma se completa con lo dispuesto en el mismo artículo 7 IX del Marco Civil de Internet brasileño, cuando señala que las personas tendrán derecho al consentimiento expreso sobre la recogida, uso, almacenamiento y tratamiento de datos personales, que deberá presentarse de forma destacada de las demás cláusulas contractuales.

Estas normas relativas al consentimiento permiten colegir que la autodeterminación informativa es parte integral del derecho a la protección de datos personales en Brasil, toda vez que serán los titulares de los datos quienes entreguen a su arbitrio su información personal a menos que la ley disponga lo contrario.

Ahora bien, el artículo 1 de la LGPD establece como objetivo de esta normativa la protección a los derechos fundamentales de libertad y privacidad y el libre desarrollo de la personalidad de la persona natural. Y a continuación el artículo 2 de la norma citada señala que la disciplina de protección de datos personales se basa en: el respeto por la privacidad; la autodeterminación informativa; la libertad de expresión, información, comunicación y opinión; la inviolabilidad de la intimidad, el honor y la imagen; el desarrollo e innovación económica y tecnológica; la libre empresa, libre competencia y protección del consumidor; y los derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por personas naturales. Asimismo, el artículo 17 del LGPD antes revisado determina que "toda persona natural tiene asegurada la titularidad de sus datos personales y garantizados los derechos fundamentales de libertad, de intimidad y de privacidad, en los términos de esta Ley".

De lo transcrito podemos concluir que existen varias referencias directas a la autodeterminación informativa como derecho autónomo, parte del contenido esencial del derecho a la protección de datos personales y en su relación con otros derechos fundamentales, artículo 2 de la LGPD. Pero además, el artículo 17 de la LGPD hace alusión a la titularidad de una persona de su dato, de esta forma se le está atribuyendo poderes de decisión, control (autodeterminación informativa) que permiten la garantía de los otros derechos citados.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

Nuevamente, la norma que recoge la prohibición de recabar datos personales sin autorización de titular es el artículo 7 VII del Marco Civil de Internet brasileño, señalando que solo será posible esta recogida si la ley lo faculta. Asimismo, el citado

artículo 7 VIII determina que la información personal solo podrá ser utilizada para finalidades que no estén prohibidas por ley.

Por su parte, el artículo 10 de la norma mencionada admite que la custodia y entrega de los registros de conexión y de acceso a aplicaciones de Internet, así como de los datos personales y del contenido de las comunicaciones privadas, atenderán a la preservación de la intimidad, de la vida privada, de la honra y de la imagen de las partes directa o indirectamente involucradas. Así, el proveedor responsable de la custodia solamente será obligado a entregar los registros mencionados en el artículo, de forma autónoma o asociados a datos personales u otras informaciones que puedan contribuir a la identificación del usuario o del terminal, mediante orden judicial. En este caso, la ley determina la excepción de la orden judicial para la entrega de información, aunque no menciona el tratamiento, sin embargo, llama la atención esta excepción que debe ser analizada puesto que permite la primera fase del procesamiento, esto es la recogida de datos personales.

Como se analizó precedentemente, las autoridades administrativas competentes para recabar información personal también necesitan de autorización legal para solicitar datos de registro que contengan información personal, filiación y dirección, de acuerdo con la ley.

Finalmente, la ley aplicable será la brasileña de conformidad con lo dispuesto en el artículo 11 del Marco Civil de Internet, según la cual cualquier operación de recolección, almacenamiento, protección o tratamiento de registros, datos personales o de comunicaciones por proveedores de conexión y de aplicaciones de internet en las que se recojan datos en el territorio nacional y el contenido de las comunicaciones, una de las terminales se localice en Brasil, entre otras causas descritas en la citada norma, facultan obligatoriamente a respetar la legislación brasileña.

Concordante con lo dispuesto en el Marco Civil de Internet, el artículo 4 de la LGPD establece que no será aplicable la regulación sobre procesamiento de datos personales cuando sea realizado: por una persona física, con fines exclusivamente privados y no económicos; para fines únicamente periodísticos y artísticos; para fines académicos, siempre y cuando se aplique el test de legitimidad, es decir, se verifique el cumplimiento de lo dispuesto en los artículos 7 y 11 relativos al procesamiento de datos personales y de datos sensibles, respectivamente. Asimismo, está excluido del régimen de protección el tratamiento realizado con fines exclusivos de: seguridad pública; defensa nacional; seguridad del estado; o investigación y enjuiciamiento de delitos penales; o proveniente de fuera del territorio nacional, siempre que el país de procedencia proporcione un grado de protección de datos personales adecuado a las disposiciones de esta Ley.

Los Párrafos 1 y 2 del citado artículo precisan que cuando se procesen datos personales con fines de seguridad pública, este no podrá realizarse por parte de un privado, se regirá por legislación específica que pondere derechos y aplique mecanismos técnicos proporcionales para satisfacer estrictamente un interés público. Además, estará sujeto al debido proceso legal, principios generales de protección y a los derechos del titular previstos en esta Ley. Esta norma es sustancial para garantizar un adecuado control de la actuación de uno de los mayores responsables de tratamiento que es el Estado, de esta forma se intenta evitar transgresiones asociadas al control social o político y en

consecuencia solo podrán tratarse datos con fines de seguridad cuando no se atente contra los derechos de los titulares o se cause discriminación.

De lo citado se colige que la norma brasileña establece un test de legitimidad a la sazón del modelo europeo, ya que, el artículo 7 de la LGPD determina que el tratamiento de datos personales solo podrá ser realizado en las siguientes hipótesis: consentimiento del titular; cumplimiento de obligación legal; ejercicio de competencias de la administración pública, previstas en leyes y reglamentos o respaldadas en contratos, convenios o instrumentos; realización de estudios de investigación, siempre que sea posible, la anonimización de los datos personales; cuando sea necesario para la ejecución de un contrato o de procedimientos precontractuales; para ejercicio de derechos en el ámbito judicial, administrativo o arbitral; para la protección de la vida o integridad física del titular o de tercero; para la tutela de la salud; para atender intereses legítimos del controlador o de tercero, excepto en el caso de prevalecer derechos y libertades fundamentales del titular; o para la protección del crédito.

La primera normativa latinoamericana que incluye como requisito para el procesamiento de datos personales al interés legítimo es la brasileña. Por lo que su alcance y delimitación consta específicamente desarrollado en el artículo 10 de la LGPD que establece que el "legítimo interés del controlador sólo podrá fundamentar el tratamiento de datos personales para fines legítimos, considerados a partir de situaciones concretas", que incluyen, pero no se limitan al apoyo y promoción de actividades del controlador o a la protección al titular del ejercicio regular de sus derechos o la prestación de servicios que lo beneficien. La norma además establece un régimen reforzado cuando se invoca este requisito como habilitante para el tratamiento, ya que: solo podrán tratarse los datos personales estrictamente necesarios para la finalidad pretendida; deberá adoptarse medidas para garantizar la transparencia del tratamiento; y, la autoridad nacional podrá solicitar al controlador informe de impacto a la protección de datos personales, observando los secretos comerciales e industriales.

En la normativa europea, el interés legítimo, ha sido ampliamente cuestionado debido a la ambigüedad del término que puede ser invocado por un responsable que a su entender puede considerar como legítimo cualquier interés. La normativa brasileña intenta definir y acotar el contenido del interés legítimo pero cuando lo asocia al *apoyo y promoción de las actividades del controlador* ha dejado nuevamente en indeterminación este concepto. Ya que, un responsable de tratamiento tendría puerta abierta para eludir el cumplimiento de una adecuada recolección y tratamiento de datos personales. Pues, podría argumentar que tal o cual actividad, como el marketing digital, por ejemplo, le permite la promoción de sus actividades y de esta manera soslayar al consentimiento que ha sido siempre la piedra de choque en estos temas.

Dentro de los vetos dispuestos a la versión original de la LGPD, está el relativo a los datos de salud, por los cuales no se necesita de consentimiento y pueden procesarse este tipo de datos no solo por profesionales de la salud y entidades de salud como señalaba el texto inicial, sino también por servicios de salud o autoridades de salud, artículo 7 sobre requisitos para el procesamiento de datos personales y artículo 11 relativo al tratamiento de datos personales sensibles. Esta incorporación se justifica en el interés vital del titular, de una expedita y eficiente prestación de servicios de salud y farmacéuticos, incluidos el diagnóstico y la terapia.

Se debe relevar que, una de las peticiones entregada en las audiencias participativas de elaboración de la Ley fue acogida pues se incorporó en la versión final del texto, la prohibición a los operadores de planes de salud privados del manejo de datos confidenciales. De este modo, se evita que el tratamiento de datos confidenciales lleve a la denegación del acceso o al "aumento injustificado de la atención médica"[1180].

De esta manera, el texto final recogido en el párrafo 4 del artículo 11 de la LGPD es el siguiente:

> Se prohíbe la comunicación o el uso compartido entre los controladores de datos personales sensibles a la salud con el fin de obtener una ventaja económica, sobre todo en cuando se van a usar los datos en los supuestos descritos en el párrafo 5 de este artículo, excepto en el caso de la prestación de servicios de salud, asistencia farmacéutica y atención médica, incluidos los servicios auxiliares de diagnóstico y terapia, en beneficio de los intereses del interesado, y para permitir: portabilidad de datos cuando lo solicite el titular; o las transacciones financieras y administrativas resultantes del uso y la prestación de los servicios mencionados en este párrafo.

Adicionalmente, se incluye el nuevo citado párrafo No. 5 que prohíbe expresamente "a los operadores de planes privados de atención médica procesar datos de salud para la práctica de selección de riesgos en la contratación de cualquier modalidad, así como en la contratación y exclusión de beneficiarios".

Finalmente, para el tratamiento de datos personales por parte de la función pública, la normativa brasileña establece un capítulo específico, el Capítulo IV denominado del tratamiento de datos personales por parte del sector público, cuyo artículo 23 establece las reglas para que las personas jurídicas de derecho público en aras del interés público o del cumplimiento de obligaciones legales, o del ejercicio de competencias, puedan tratar datos personales de sus ciudadanos.

Para lo cual se han establecido varias reglas que obligan a las autoridades a proporcionar informaciones claras y actualizadas sobre: la previsión legal, la finalidad, los procedimientos, las prácticas utilizadas para la ejecución de esas actividades; la indicación de quien es el encargado, los términos y procedimientos para el ejercicio de los derechos del titular contra las autoridades públicas "observando las disposiciones de la legislación específica, en particular las disposiciones de la Ley Nº 9.507, de 12 de noviembre, 1997 (la Ley de *Habeas Data*) , la Ley N ° 9784 de 29 de enero de 1999 (Ley general de procedimiento Administrativo) , y la Ley N ° 12.527, de 18 de noviembre, 2011 (Ley de Acceso a la Información)"; y además, la obligación de proveer de dicha información en vehículos de fácil acceso, preferentemente en sus sitios web.

Esta norma además de establecer deberes de información específicos para el sector público, señala el límite de la actuación del sector público respecto de los datos personales de sus ciudadanos, añadiéndose que los artículos 24, 25, 26, 27 y 29 establecen una serie de normas aplicables al intercambio de información entre instituciones públicas. Finalmente, el artículo 30 determina que la autoridad nacional podrá establecer normas complementarias para las actividades de comunicación y de

[1180] "Se sanciona una ley que crea la Autoridad Nacional de Protección de Datos", E-Health Reporter Latinoamérica, accedido el 22 de agosto de 2019, en https://ehealthreporter.com/es/noticia/se-sanciona-una-ley-que-crea-la-autoridad-nacional-de-proteccion-de-datos/

uso compartido de datos personales, de esta manera se reconoce la especialidad y jerarquía superior de la norma de protección de datos respecto de normativas relativas a interoperabilidad.

En el numeral IV del artículo 23 se incluye otro veto, relativo a la prohibición a las autoridades públicas de compartir con otros organismos públicos o entidades jurídicas de derecho privado, los datos personales de aquellas personas solicitantes que hayan accedido a información a través del ejercicio de la Ley de Acceso a la Información. La razón del veto atiende a que la entrega de este tipo de datos "crea inseguridad jurídica, […] el acceso público es una medida recurrente y esencial para el ejercicio regular de diversas actividades y políticas públicas". De esta manera, la difusión de la identidad de las personas que ejercen este derecho de acceso pudiera afectar la transparencia o el ejercicio de facultades de control.

d. Principios

i. Deber de información

Como se ha señalado en varias ocasiones el derecho a la información conlleva la obligación de los responsables de los ficheros de cumplir con su deber de información. Desde esta perspectiva, el artículo 7 VIII del Marco Civil de Internet señala la obligación de los proveedores de entregar información clara y completa sobre la recogida, uso, almacenamiento, tratamiento y protección de sus datos personales.

El artículo 7º XI del Marco Civil de Internet indica entre los derechos que tiene la ciudadanía cuando accede a internet, la publicación y claridad de las eventuales políticas de uso por parte de los proveedores de conexión a internet y de las aplicaciones de internet. Esta información debe estar disponible también como garantía de los derechos de consumidor.

Ahora bien, el numeral VI del artículo 6 de la LGPD señala entre los principios aplicables al procesamiento de las actividades de datos personales, el de transparencia, por el cual se garantiza a los titulares, información clara, precisa y de fácil acceso sobre el tratamiento y los agentes tratantes, observando los secretos comerciales e industriales. Destacándose su adaptación al RGDP, ya que incluso el principio se denomina transparencia en lugar de información. De este breve concepto se concluye que a través del principio de transparencia se garantiza la efectiva vigencia del derecho de información. Así como, debe recalcarse el reconocimiento expreso a los límites de la información estos son los secretos comerciales e industriales, parte del sistema de propiedad intelectual.

ii. Pertinencia

El artículo 13 de Reglamento al Marco Civil de Internet referente a seguridad señala que los proveedores de conexión y de aplicación que custodian, almacenan y tratan datos personales y comunicaciones privadas están obligados a cumplir con varios estándares de seguridad. Entre ellos, la obligación de retener la menor cantidad posible de datos personales, comunicaciones privadas y registros de conexión y acceso a aplicaciones, los cuales deberán ser excluidos tan pronto se haya alcanzado la finalidad de su uso o cuando se haya concluido el plazo fijado por obligación legal. De esta

forma, se garantiza desde una perspectiva técnica de seguridad, la pertinencia temporal y de fondo de los datos personales en un determinado fichero.

El artículo 6 de la LGPD señala que el tratamiento de datos personales observará, además de la buena fe, el principio de adecuación, que es la "compatibilidad del tratamiento con las finalidades informadas al titular, de acuerdo con el contexto del tratamiento". De la comparación con las normativas regionales, este concepto resulta el más claro ya que determina el alcance de la pertinencia asociado a la finalidad del tratamiento y no a la calidad del dato.

iii. Calidad

Conforme determina el numeral V del artículo 6 de LGPD, el procesamiento de datos personales deberá respetar la buena fe y el principio de calidad de datos, que consiste en la garantía de precisión, claridad, relevancia y actualización de los datos, de acuerdo con la necesidad y para el cumplimiento del propósito de su procesamiento. En este concepto es necesario relevar la relación entre la calidad del dato y la finalidad del tratamiento lo que permite contextualizar los datos personales, pero además son importantes características como la claridad y la precisión que hacen alusión a la veracidad del dato, criterio generalmente aceptado para definir este principio.

El numeral X del artículo 7 del Marco Civil de Internet ha sido enmendado por la LGPD en sus disposiciones reformatorias y establece que se debe producir la eliminación definitiva de los datos personales que se ha proporcionado a una aplicación de Internet, en particular a solicitud suya, al final de la relación entre las partes, excepto en el caso de la custodia obligatoria de los registros previstos en esta Ley.

Adicionalmente, el artículo 50 de la LGPD señala que el controlador, "observando la estructura, escala y volumen de sus operaciones, así como la sensibilidad de los datos procesados y la probabilidad y gravedad del daño a los interesados", puede ordenar la actualización constante con base en la información obtenida del monitoreo continuo y de evaluaciones periódicas. Esta buena práctica tiene como finalidad cumplir con el principio de calidad de dato. Su finalidad es doble pues, además de evitar posibles transgresiones a las personas también permite que los resultados del tratamiento realizado por el agente sean óptimos para los fines definidos previamente.

iv. Finalidad

Acerca del principio de finalidad, este se encuentra recogido en el Capítulo II, "De los derechos y garantías de los usuarios", en el artículo 7 VIII del Marco Civil de Internet brasileño. Dicha norma señala el derecho de los ciudadanos y usuarios a recibir información clara y completa sobre la recogida, uso, almacenamiento, tratamiento y protección de sus datos personales, que solo podrán ser utilizados para finalidades que justifiquen su recolección, que no estén prohibidas por ley; y además queden especificadas en los contratos de prestación de servicios o en los términos de uso de las aplicaciones de internet.

El artículo 6 de la LGPD señala entre los principios aplicables al tratamiento de datos personales al propósito, que es la "realización del tratamiento para propósitos legítimos,

específicos, explícitos e informados al titular, sin posibilidad de tratamiento posterior de forma incompatible con esas finalidades".

De modo que la finalidad como principio se encuentra garantizada en la normativa brasileña; toda vez que el propósito debe estar debidamente justificado, cumplirse con un estricto principio de legalidad y esté claramente establecida para no tener equívocos en el contenido de los contratos de servicios entre proveedores y usuarios, tal como señala el Marco Civil de Internet. Pero principalmente, son condiciones indispensables para un tratamiento adecuado la legitimidad de la finalidad y su información al titular porque a través de ellas se garantiza el principio de pertinencia y se otorga contexto a los datos en aras de su calidad, en suma se garantiza la buena fe del responsable del tratamiento. Adicionalmente, la precisión sobre la imposibilidad de tratamiento posterior si las nuevas finalidades son incompatibles son disposiciones normativas que controlan la lealtad de quien trate los datos.

v. Seguridad

El Reglamento al Marco Civil de Internet en el artículo 13 señala que los proveedores de conexión y de aplicación cuando custodien, almacenen o traten datos de personas y comunicaciones privadas, deben observar una serie de estándares de seguridad: control estricto de acceso, definición de las personas con privilegios de acceso, previsión de mecanismos de autenticación, creación de inventario de acciones, encriptación o medidas equivalente, estándares técnicos y operativos, entre otros.

En el mismo reglamento consta también el artículo 16, el cual señala la obligación de difundir de forma clara y accesible, usando los propios sitios de internet, los estándares de seguridad para que los proveedores de aplicación y de conexión puedan cumplimentar.

Uno de los temas más desarrollados en la LGPD brasileña es el principio de seguridad. Reconocido en el numeral VII del artículo 6 de la LGPD que lo define como la: "utilización de medidas técnicas y administrativas capaces de proteger los datos personales de accesos no autorizados y de situaciones accidentales o ilícitas de destrucción, pérdida, alteración, comunicación o difusión".

El Capítulo VII denominado Seguridad y buenas prácticas recoge dos secciones, la Sección I, sobre seguridad y confidencialidad de los datos y la Sección II, sobre buenas prácticas y gobernanza. Esta propuesta normativa nos demuestra que la seguridad se ha vuelto una de las mayores problemáticas en el tratamiento de datos personales, de tal manera que el modelo ha mudado de la simple visión de los datos personales a los que hay que proteger porque son activos valiosos para la empresa a un modelo en el que a través de la seguridad protejo a los titulares de los datos y permito el ejercicio de sus derechos fundamentales.

La importancia de la seguridad ha dejado de ser exclusivamente económica y se ha trasladado al plano de la responsabilidad frente a los titulares de los datos, a quienes no solo se les deberá indemnizar en el caso de incumplimientos sino que se deberá arbitrar todos los esfuerzos y diligencias, ya sean estas preventivas, durante o incluso con posterioridad al tratamiento de sus datos personales.

En este sentido, el artículo 46 de la LGPD señala que:

> […] los agentes de tratamiento, controladores y operadores deben adoptar medidas de seguridad, técnicas y administrativas aptas para proteger los datos personales de accesos no autorizados y de situaciones accidentales o ilícitas de destrucción, pérdida, alteración, comunicación o cualquier forma de tratamiento inadecuado o ilícito.

Esta nueva visión integral, se concibe a la seguridad no solo en el ámbito técnico, sino incluso en el administrativo frente a realidades previstas o incluso imprevistas.

Adicionalmente, el artículo 48 de la LGPD establece que la Autoridad de control nacional asume entre sus responsabilidades la de establecer normas técnicas mínimas de seguridad que deberán ser implementadas por los agentes de tratamiento, desde el diseño del producto y para la ejecución del servicio tomando en cuenta la naturaleza de la información, las características específicas del tratamiento y el estado actual de la tecnología, en especial el caso de los datos personales sensibles.

Respecto de la notificación de vulneraciones, el artículo 48 del LGPD, señala que el controlador deberá comunicar en un plazo razonable a la autoridad nacional y al titular la ocurrencia de un incidente de seguridad que pueda acarrear riesgo o daño relevante a los titulares. Para lo cual, se mencionará como mínimo, la descripción de la naturaleza de los datos personales afectados; los titulares implicados; las medidas técnicas y de seguridad utilizadas; los riesgos relacionados con el incidente; los motivos de la demora, si la comunicación no fue inmediata; y las medidas de reversión o mitigación del daño.

Adicionalmente, la autoridad nacional verificará la gravedad del incidente y podrá dictar salvaguardas adicionales, tales como: una amplia divulgación del hecho en medios de comunicación; y medidas para revertir o mitigar los efectos del incidente.

El artículo 50 de la LGPD señala que para el tratamiento de datos personales es facultativo de los controladores y operadores:

> […] formular reglas de buenas prácticas y gobernanza que establezcan las condiciones de organización, el régimen operativo, el procedimientos, incluidas las quejas y peticiones de los titulares, normas de seguridad, normas técnicas, obligaciones específicas para las diversas partes involucradas en el procesamiento, acciones educativas, mecanismos internos de supervisión y mitigación de riesgos y otros aspectos relacionados con el procesamiento de datos personal.

Es decir, a través de estas buenas prácticas y sistemas de gobernanza, además de establecer mínimos que eviten vulnerabilidades, se cumple otro de los objetivos de la implementación de esta visión integral de seguridad, que es la construcción de mecanismos transparentes y participativos que permitan afianzar una relación de confianza entre los agentes de tratamiento y los titulares de los datos personales.

vi. Consentimiento

Conforme señala el artículo 7 VII del Marco Civil de Internet brasileño, solo si existe consentimiento libre, expreso e informado o en circunstancias establecidas por la ley se puede entregar datos personales a un tercero.

El mismo artículo 7 IX del Marco Civil de Internet brasileño determina, además, que este consentimiento expreso sobre la recogida, uso, almacenamiento y tratamiento de datos personales deberá presentarse de forma destacada de las demás cláusulas contractuales, especialmente en relaciones de consumidor.
Se colige que, para que opere el principio de consentimiento, el titular debe estar debidamente informado. Además, a través de las autorizaciones que otorga el titular se viabiliza el ejercicio del derecho a la autodeterminación informativa.

Estas características del consentimiento se encuentran plenamente vigentes en el artículo 8 de la LGPD puesto que, el consentimiento deberá referirse a fines determinados, que deberán ser puestos en conocimiento del titular y debidamente comprendidos por este, de tal manera que las autorizaciones genéricas para el tratamiento de datos personales serán nulas. Por lo que, de existir vicios del consentimiento, como el haber sido obtenido a través de engaños o de forma abusiva o no haberse presentado previamente con transparencia, de forma clara e inequívoca, el tratamiento queda vedado por considerarse a este consentimiento nulo y sin efecto, artículo 9 LGPD.

Más aún, la condición del consentimiento es que este debe ser proporcionado por escrito o por otro medio que demuestre manifestación de voluntad del titular. Si es por escrito, constará en cláusula contractual destacada. Tomando en cuenta que, corresponderá al controlador la carga de la prueba de que el consentimiento fue obtenido de conformidad con lo dispuesto en esta Ley.

Finalmente, el consentimiento puede ser revocado en cualquier momento, por manifestación expresa del titular, sobre todo si han existido modificaciones a las condiciones iniciales con las que este fue emitido, artículo 8 y 9 de la LGPD. Es decir, la revocatoria es una de las prerrogativas del derecho a la autodeterminación informativa.

vii. Libre acceso:

Este principio se reconoce exclusivamente en el artículo 6 de la LGPD que establece al libre acceso, como la "garantía que faculta a los titulares, de una consulta facilitada y gratuita, la forma y la duración del tratamiento, así como sobre la totalidad de sus datos personales".

Este contenido se replica en el artículo 9 de la LGPD que establece los criterios para el ejercicio del derecho de acceso por los cuales se deberán disponibilizar de forma clara, adecuada y ostensiva la siguiente información: propósito específico del tratamiento; forma y duración del tratamiento, observados los secretos comerciales e industriales; identificación del controlador; información de contacto del controlador; información sobre el uso compartido de datos por el controlador y el propósito; responsabilidades de los agentes que realizarán el tratamiento; y derechos del titular, con mención explícita a los derechos contenidos en el art. 18 de esta Ley.

De esta manera consideramos que existe una íntima relación entre el principio de transparencia, el de libre acceso y el derecho de acceso, tanto más que en todos ellos se hace alusión a la información que el agente de tratamiento debe poner en conocimiento de un titular. Ahora bien, consideramos que lejos de aportar claridad, la incorporación

de este principio confunde el alcance del principio de transparencia y del derecho de acceso. Así como, pareciera que pudiera entrar en conflicto con aquellas disposiciones que establecen limitaciones temporales a las solicitudes de acceso a información o a la portabilidad de los datos de un titular.

viii. Prevención:

Un principio nuevo, propio de la normativa brasileña es el reconocido en el numeral VIII del artículo 6 que señala a la prevención como la "adopción de medidas para prevenir la ocurrencia de daños en virtud del tratamiento de datos personales".

Este principio no se desarrolla en el resto del texto, únicamente en el capítulo sobre seguridad se aprecia una postura preventiva, por lo que pareciera que este es un principio cuyo mayor desarrollo se plantea desde esta perspectiva. Ahora bien, los principios reconocidos en el artículo 6 de la LGPD son en realidad medidas, de toda índole, destinadas a prevenir posibles daños, definición propia del citado principio de prevención.

ix. No discriminación:

Otro de los principios propios de la normativa brasileña está reconocido en el numeral IX del artículo 6 que determina a la no discriminación: como la imposibilidad de realización del tratamiento para fines discriminatorios ilícitos o abusivos.

El concebir a la no discriminación como principio y volverlo un mandato de optimización que rige de manera general, en el diseño y ejecución de cualquier forma de tratamiento de datos personales es motivo suficiente por el cual considero que se lo concibió como principio y no únicamente como prohibición específica.

Asimismo, el artículo 21 de la LGPD determina que los datos personales referentes al ejercicio regular de derechos por parte del titular no pueden ser utilizados en su perjuicio. Esta norma es una aplicación práctica del principio de no discriminación, pues no pueden utilizarse en su contra los propios datos del titular relativos al ejercicio de sus derechos, ya que además de transgredir la dignidad del titular, su indebida utilización podría mermar el uso de estos mecanismos de cumplimiento de derechos y por ende de aplicación del debido proceso.

x. Responsabilidad y rendición de cuentas:

El numeral X del artículo 6 de la LGPD señala como principio el de responsabilidad y rendición de cuentas, que consiste en la demostración, por el agente, de la adopción de medidas eficaces y capaces de comprobar la observancia y el cumplimiento de las normas de protección de datos personales e incluso de la eficacia de esas medidas.

Si bien este principio hace alusión a rendición de cuentas más que a la asunción de responsabilidad. Encontramos en el artículo 42 de la LGPD al principio de responsabilidad desarrollado ya que determina que, si en razón del tratamiento de datos personales, se ha causado un daño patrimonial, moral, individual o colectivo, en violación a la legislación de protección de datos personales, el agente de tratamiento

está obligado a reparar. Además, se reconoce la responsabilidad solidaria entre controlador y operador cuando este último incumple las obligaciones legales, no ha seguido las instrucciones lícitas del controlador o no ha mantenido criterios de seguridad.

De esta manera, tanto la rendición de cuentas como la responsabilidad, en sí misma, son parte del sistema de protección de los datos personales, dotando a los titulares de herramientas para fiscalizar la actuación de un agente de tratamiento, así como para exigir la reparación de los daños que su inadecuada actuación pudiera haber causado.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

i. Derecho de acceso

El derecho de acceso se materializa mediante el *habeas data* contenido en el artículo 5 de la Constitución brasileña, el cual permite el conocimiento de informaciones relativas a la persona que constan en registros o bancos de datos de entidades gubernamentales o de carácter público.

Asimismo, el artículo 10 del Marco Civil de Internet señala que la custodia y entrega de los datos personales y del contenido de las comunicaciones privadas deben atender a la preservación de la intimidad, de la vida privada, de la honra y de la imagen de las partes directa o indirectamente involucradas. De esta forma, para garantizar estos derechos fundamentales se ha establecido que solo se entregará información personal sin autorización del titular con orden judicial o disposición legal previa.

Por su parte, el Reglamento al Marco Civil de Internet señala, en el artículo 15, la obligación de mantener en formato interoperable y estructurado los datos catastrales, es decir, los relativos a la filiación, la dirección y la calificación personal, entendida como nombre, prenombre, estado civil y profesión del usuario. Esto con la finalidad de facilitar el acceso técnico y seguro resultante de la decisión judicial o la determinación legal.

Asimismo, los artículos 11 y 12 del citado reglamento, establecen que las autoridades administrativas a que se refiere el artículo 10, § 3º de la Ley 12.965, de 2014, Marco Civil de Internet, podrán acceder a datos catastrales cuando sean competentes, tengan fundamento legal que los faculte y motivación suficiente que sustente su solicitud de acceso.

En el artículo 11 § 3 del reglamento en mención, se establece que las solicitudes de acceso deberán especificar a los individuos cuyos datos están siendo requeridos y la información deseada, siendo vedadas solicitudes colectivas que sean genéricas o inespecíficas.

Finalmente, el artículo 12 del reglamento determina que la autoridad máxima de cada órgano de la administración pública federal publicará anualmente en su sitio en internet informes estadísticos de solicitud de datos catastrales que contendrá: el número de solicitudes realizadas; la lista de los proveedores de conexión o de acceso a las

aplicaciones a las que se requieran los datos; el número de solicitudes concedidas y denegadas por los proveedores de conexión y de acceso a las aplicaciones; el número de usuarios afectados por tales solicitudes.

Cuando los datos de los cuales se solicita acceso son aquellos denominados catastrales, deberán realizar una solicitud que cumpla lo dispuesto en los artículos 11 y 12 del reglamento a la Ley de Marco Civil de Internet.

Respecto de los datos personales y comunicaciones privadas custodiados y entregados a proveedores privados, estos podían ser exigidos únicamente por sus titulares, y en cuanto a terceros se necesita de una orden judicial o disposición legal.

Antes de la entrada en vigencia de la LGPD, la persona natural solo podía acceder a bases públicas mediante *habeas data.*

Actualmente, el artículo 18 de la LGPD establece que el titular de los datos personales tiene derecho a obtener del controlador, en cualquier momento y mediante solicitud: la confirmación de la existencia de tratamiento; el acceso a sus datos; deberá informar de manera inmediata a los otros agentes de tratamiento con los que haya realizado uso compartido de datos la corrección, eliminación, anonimización o bloqueo de los datos, para que repitan idéntico procedimiento.

El citado artículo 18 también señala los casos en que el agente de tratamiento puede negarse al pedido de acceso: cuando éste no ha tratados los datos pero deberá indicar, siempre que sea posible, la identidad del que lo esté realizando; o, las razones de hecho o de derecho que le han impedido cumplir con la solicitud. La petición será atendida sin costo para el titular.

Asimismo, el artículo 19 señala que el responsable está en la obligación de confirmar la existencia o el acceso a datos personales, previa solicitud del titular, en formato simplificado, de forma inmediata; por medio de una declaración clara y completa, que indique el origen de los datos, los criterios de tratamiento utilizados y su finalidad, en el plazo de hasta 15 días contados de la fecha de la solicitud del titular. Además dicha norma aclara que, los datos personales serán almacenados en formato que favorezca el ejercicio del derecho de acceso y podrán ser suministrados, a criterio del titular por medio electrónico, seguro e idóneo para ese fin; o en forma impresa.

De lo dispuesto anteriormente, se colige que el derecho de acceso ha sido debidamente configurado en la LGPD pues se han delineado con claridad los derechos del titular, las obligaciones de los agentes de tratamiento, las excepciones que los cobijan y los mecanismos de cumplimiento. Y con ello, nuevamente existe un nivel adecuado de protección conforme el estándar europeo.

Finalmente, como referimos líneas arriba el artículo 6 de la LGPD, determina el principio de libre acceso que está directamente relacionado con el derecho de acceso, pues precisamente determina la gratuidad y la alusión expresa a la entrega de la totalidad de los datos personales de un titular. Si se lo ha concebido como principio y no como derecho es precisamente para que se convierta en un mandato de optimización que pueda aplicarse de manera general, no solo para el derecho de acceso.

ii. Derecho de rectificación

Consta en el artículo 5 LXXII de la Constitución de la República Federativa del Brasil de 1988 que se concederá *habeas data* a brasileños y extranjeros residentes en el país para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo. Esta acción permite cumplir uno de los elementos esenciales del derecho a la protección de datos personales, esto es la modificación de datos personales. Pero, además, llama la atención que la norma establezca otra posibilidad: iniciar procedimiento secreto, judicial o administrativo.

Ahora, el vigente artículo 18 de la LGPD establece que el titular de los datos personales tiene derecho a obtener del controlador, en cualquier momento y mediante solicitud: la corrección de datos incompletos, inexactos o desactualizados.

Coincide con este derecho lo dispuesto en el artículo 6 numeral V relativo al principio de calidad de los datos, por el cual los agentes de tratamiento deberán garantizar a los titulares de los datos precisión, claridad, relevancia y actualización de los datos, para lo cual será necesario que en el caso de inexactitud, desactualización u obsolescencia se arbitren los canales para el titular pueda solicitar su derecho de rectificación.

Finalmente, el citado artículo 18 prevé que el responsable debe informar inmediatamente a los agentes de tratamiento con los que ha compartido datos sobre la corrección para que repitan el mismo procedimiento, excepto si se demuestra que la comunicación es imposible o conlleva un esfuerzo desproporcionado.

iii. Derecho de oposición

Ni en la Constitución, ni en la ley, ni en el reglamento de Marco Civil de Internet consta expresamente el derecho de oposición; sin embargo, se puede colegirlo en el ejercicio del principio de consentimiento contenido en los artículos 7 VII y IX y, especialmente, en el 16 del Marco Civil de Internet brasileño que dice:

> Artículo 16. En la provisión de conexión, onerosa o gratuita, está prohibida la custodia: I – de los registros de acceso a otras aplicaciones de Internet sin que el titular de los datos haya consentido previamente, respetando lo dispuesto en el artículo 7º; y II – de datos personales que sean excesivos en relación a la finalidad para la cual fue dado el consentimiento por su titular.

Para comprender el alcance del contenido de las normas en cuestión, así como comprender los cambios provocados por el Marco Civil de Internet brasileño, Claudio Nazareno, consultor legislativo del área XIV – ciencia y tecnología, comunicaciones e informática, señala en su texto que figura como antecedente a la normativa en cuestión, lo siguiente:

> [...] sólo se pueden recoger datos con el consentimiento previo del usuario y sólo aquellos que no son excesivos en relación con la finalidad de la recogida. El usuario tendrá que dar su consentimiento expreso para recoger sus hábitos de navegación, sin embargo, en algunas situaciones, puede no tener la opción de continuar utilizando el

> servicio si no acepta los términos dictados por el sitio. Recogidas abusivas (por ejemplo, compras hechas recogidas por sitios de noticias) están prohibidas.[1181]

Así se colige que existe prohibición expresa en la recogida de datos sin consentimiento del titular, lo que en suma significa que al menos en el momento de la captación existe un nivel de oposición.

Ahora bien, la vigente LGPD, señala expresamente en el artículo 18 párrafo 2º que el titular podrá oponerse al tratamiento realizado en base a una de las hipótesis de dispensa del consentimiento, o en caso de incumplimiento a lo dispuesto en esta Ley.

No existe claridad sobre lo que significa la dispensa del consentimiento o la renuncia al consentimiento que es otra forma de traducir esta condición propia del derecho de oposición. Y es que, al no existir una determinación de su significado solo resta interpretar el artículo 7 que señala como primer criterio para el procesamiento de datos personales al consentimiento, por lo que los otros requisitos determinados en este artículo serían aquellos en los que la voluntad del titular no entra en discusión y por ende no es aplicable ni el consentimiento ni el derecho de oposición, ya que la ley ha ponderado los casos en los que aun en ausencia de autorización y por ende, aun en contra de la voluntad de oponerse por parte del titular, pueden ser tratados datos personales.

Ahora bien, la alusión al incumplimiento a lo dispuesto en esta Ley como criterio para aplicar la oposición nuevamente es aplicable en aquellos casos de procesamiento autorizados por el titular, porque de aquellos que tienen otro criterio de legitimación solo podrían solicitarse el acceso, la rectificación o la eliminación cumpliendo los requisitos señalados en cada caso.

Finalmente, el numeral III del artículo 15 de la LGPD señala entre los casos de conclusión del procesamiento de datos personales a la revocatoria por parte del titular, mediante manifestación expresa de su negativa de consentimiento, en cualquier momento, siempre que lo existan causales que lo impidan como las contempladas en el artículo16 de la LGPD. Es decir, se puede evidenciar el derecho de oposición a través de la revocatoria del consentimiento prevista en el citado artículo 15 de la LGPD que impide que un agente siga tratando datos personales de un titular.

iv. Derecho de cancelación

El derecho de cancelación o eliminación consta en el artículo 7 X de la Ley de Marco Civil de Internet que textualmente dice:

> Artículo 7º El acceso a Internet es esencial para el ejercicio de la ciudadanía y para los usuarios están garantizados los siguientes derechos: [...] X – la eliminación definitiva de los datos personales que se hayan proporcionado a determinada aplicación de Internet, a solicitud suya, al término de la relación entre las partes, salvo en los casos de custodia obligatoria de registros previstas en esta ley;

[1181] Brasil, Marco Civil Brasileño de Internet en Español, *Ley 12.965*, de 23 de abril de 2014, que establece los principios, garantías, derechos y deberes para el uso de Internet en Brasil.

Del contenido citado se desprende que la eliminación únicamente procede solo en el caso de terminación de la relación, lo que podría contradecir tanto al derecho de oposición del dato como al contenido de la eliminación, que en otras legislaciones procede por la simple petición del solicitante sin necesidad de demostrar supuesto alguno.

Actualmente, el vigente artículo 18 de la LGPD establece que el titular de los datos personales tiene derecho a obtener del controlador, en cualquier momento y mediante solicitud: la eliminación de datos innecesarios, excesivos o tratados en incumplimiento con lo dispuesto en esta Ley; la eliminación de los datos personales tratados con el consentimiento del titular, excepto en las hipótesis previstas en el art. 16 de esta Ley.

Adicionalmente, el artículo 15 de la LGPD prevé el término del tratamiento de datos personales y por ende la posibilidad de exigir su eliminación cuando: la finalidad ha sido alcanzada; los datos dejaron de ser necesarios o pertinentes al alcance de la finalidad específica anhelada; el fin del período de tratamiento.

De otro lado, el artículo 16 de la LGPD señala que los datos personales serán eliminados después del término de su tratamiento, a menos que debido "al ámbito y a los límites técnicos de las actividades", sea necesaria su conservación como en los casos que se listan a continuación: cumplimiento de obligación legal o regulatoria del controlador; estudio de investigación, siempre que sea posible, la anonimización de los datos personales; transferencia a tercero, siempre que se respeten los requisitos de tratamiento de datos dispuestos en esta Ley; uso exclusivo del controlador, vedado su acceso a terceros, y desde que los datos sean anónimos.

De esta manera se configura un derecho de eliminación visto desde distintas aristas, ya que se encuentra asociado a la condición de dato innecesario, excesivo, o tratados en incumplimiento de la Ley; pero también, al tiempo de conservación o al cumplimiento de su finalidad; y, a la revocatoria de consentimiento del titular.

El citado artículo 18 numeral IV, además del derecho de eliminación, señala los derechos al anonimato y al bloqueo cuando los datos sean innecesarios, excesivos o tratados en violación de las disposiciones de esta Ley. La anonimización se convierte en un mecanismo de protección que habilita al responsable a conservar el dato y al mismo tiempo protege al titular. En el caso del bloqueo este opera temporalmente hasta que se verifique las condiciones señaladas previamente que habilitan la eliminación permanente.

v. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

Este derecho se reconoce en el artículo 20 de la LGPD. Por el cual, el interesado tiene derecho a solicitar la revisión de aquellas decisiones tomadas únicamente sobre la base de un procesamiento automatizado de datos personales cuando estos hayan afectado sus intereses, incluidas las decisiones para definir su perfil personal, profesional, de consumo y de crédito, o los aspectos de tu personalidad.

Se obliga además a que el controlador proporcione, cuando se solicite, información clara y adecuada sobre los criterios y procedimientos utilizados para la decisión

automatizada, siempre y cuando no se afecten secretos comerciales e industriales, pero la autoridad nacional podrá realizar auditorías para verificar aspectos discriminatorios en el procesamiento automatizado de datos personales.

La versión original de esta norma, antes de la Medida Provisional 869 de 2018, señalaba que el titular tenía derecho a solicitar que personas físicas revisen las decisiones tomadas únicamente sobre la base del procesamiento automatizado. Sin embargo, el veto señaló que:

> […]La propuesta legislativa, al establecer que cualquier decisión basada únicamente en el tratamiento automatizado es susceptible de revisión humana, va en contra del interés público, ya que tal requisito hará que los modelos de planes de negocios actuales de muchas compañías, especialmente las nuevas empresas, sean inviables, así como el impacto en el análisis del riesgo de crédito y los nuevos modelos de negocio de las instituciones financieras, que tienen un efecto negativo en la oferta de crédito a los consumidores, en cuanto a la calidad de la garantía, el volumen de crédito contratado y la composición de precios, también afecta las tasas de inflación y la conducción de la política monetaria.

Es decir, se sostiene que la intervención humana en la revisión del tratamiento automatizado significa otorgarle poderes discrecionales a una determina persona, por lo que finalmente la normativa aprobada establece el derecho a solicitar revisión sin hacer alusión a que esta deba ser realizada por persona natural, por lo que podría utilizarse medios automáticos o a través del análisis humanos de considerarse necesario en ciertos contextos.

vi. Derecho de consulta al registro general de protección de datos personales

El capítulo VI sobre agentes de tratamiento de datos personales señala en la Sección I, sobre Controlador y operador, en su artículo 37 de la LGPD, la obligación de estos de mantener un registro de las operaciones de procesamiento de datos personales que realizan, especialmente cuando se basan en intereses legítimos.

A su vez, el artículo 38 de la LGPD señala que la autoridad nacional podrá exigir al controlador que elabore un informe sobre el impacto de la protección de datos personales, incluidos los datos confidenciales. Este informe contendrá como mínimo: "una descripción de los tipos de datos recopilados, la metodología utilizada para la recopilación y el aseguramiento de la seguridad de la información, y el análisis del controlador de medidas, salvaguardas y mecanismos de mitigación de riesgos adoptados".

Esta normativa no reconoce el derecho de consulta al registro general por parte del titular sino que establece únicamente la obligación de los agentes de tratamiento de mantener un registro que después será usado para control y vigilancia por parte de la autoridad nacional. Añadiéndose que, tal como propone el modelo europeo, ya no se exige que el registro se realice previamente ni a través de sistemas dispuestos, para el efecto, por parte del órgano de control, sino que estos deberán mantenerse en las propias bases del agente de tratamiento.

vii. Derecho a indemnización por daños causados

Si bien el Marco Civil de Internet menciona a la responsabilidad como uno de los principios que rigen la utilización de internet en Brasil, no existe expresa alusión frente a una indebida utilización de los datos personales de una persona que pueda generar indemnización por los daños causados. La única referencia aparece del artículo 3º de la citada ley que expresamente dice:

> Art. 3º La disciplina de la utilización de Internet en Brasil cuenta con los siguientes principios: [...] VI – fijar responsabilidad a las partes de acuerdo con sus actividades, en los términos de la ley;

El Marco Civil de Internet contiene la sección III, denominada "De la responsabilidad por daños que surgieran del contenido generado por terceros" que tampoco se refiere al uso inadecuado de datos personales, sino a la generación de contenido informativo elaborado en ejercicio de los derechos de libertad de expresión, libertad de información y comunicación, por lo que en consecuencia este contenido no se aplica a datos personales de un individuo.

Finalmente, el artículo 7º de la Ley Marco Civil de Internet señala que:

> Art. 7º El acceso a Internet es esencial para el ejercicio de la ciudadanía y para los usuarios están garantizados los siguientes derechos: I – la inviolabilidad de la intimidad y de la vida privada, asegurando su protección y la indemnización por el daño material o moral resultante de su violación;

Es decir, en la citada ley, el derecho a solicitar el pago de los daños y perjuicios causados no está asociado al derecho a la protección de datos personales, sino a los conexos intimidad y vida privada.

Ahora bien, tal como se analizó previamente cuando se revisó el principio de responsabilidad, el artículo 42 de la LGPD, señala que si alguno de los agentes de tratamiento, en el ejercicio de la actividad de procesamiento de datos personales, causa daños materiales, morales, individuales o colectivos a terceros, por violación de la legislación de protección de datos personales, estos deberán ser reparados. De esta manera, esta normativa reconoce el derecho a una indemnización por inadecuado manejo de datos personales, sin que sea necesario demostrar que se ha causado daño a la intimidad o a la vida privada sino que basta que la actuación de inadecuado tratamiento por parte del agente ha causado cualquier clase de perjuicio.

Además, la norma establece que para una adecuada determinación de la indemnización se deberá diferenciar los daños materiales de los morales, así como perjuicios individuales o colectivos, elementos que deberán ser evaluados por un juez civil.

Además, el citado artículo 42 de la LGPD ha previsto una garantía probatoria en favor de la parte indefensa en esta relación, esto es, revertir la carga de la prueba a favor del interesado cuando, "en su opinión, la alegación es probable, hay una suficiencia a los efectos de producir evidencia; o, la producción de evidencia por el interesado es excesivamente costosa".

Finamente, el párrafo 4 de la norma citada señala que toda persona que repare el daño al titular tendrá de repetición contra las otras partes responsables.

Sin duda, el establecimiento de este derecho genera un efecto de prevención general, puesto que los agentes de tratamiento cumplirán con sus obligaciones debido a la posibilidad de ser demandados civilmente. Pero además, este derecho de indemnización genera interés en el derecho a la protección de datos personales por parte de sus titulares, ya que estos ejercerán sus derechos ante la posibilidad de recibir una indemnización por el posible daño causado. Actuación que viabiliza la fiscalización, mediante el empoderamiento ciudadano, a los agentes de tratamiento públicos o privados.

viii. Derecho a la confidencialidad

Respecto a la confidencialidad de los datos personales, el artículo 10 de la Ley Marco Civil de Internet señala que la custodia y entrega de los registros de conexión y de acceso a aplicaciones de Internet, así como de los datos personales y el contenido de las comunicaciones privadas, deben atender a la protección de la intimidad, de la vida privada, de la honra y de la imagen. Por ello se prevé en el § 4º que las medidas y procedimientos de seguridad y secreto empleados por los tipos de responsables antes señalados, deben ser informados de forma clara y atenerse a patrones definidos en el reglamento, respetando su derecho de confidencialidad en lo que respecta a secretos empresariales.

Asimismo, aparece en el artículo 22 de la Ley de Marco Civil de Internet la facultad de solicitar al juez que ordene al responsable del registro de conexión o de registros de acceso a aplicaciones de internet que guarde registros con fines de investigación o instrucción probatoria. De tal forma que, conforme dispone el artículo 23 de la ley en mención, el responsable debe tomar las providencias necesarias para garantizar sigilo de la información recibida y con ello evitar transgredir el derecho a la intimidad, la vida privada, la honra y la imagen del usuario.

El artículo 15 de la Ley de Marco Civil de Internet señala además que será el proveedor de aplicaciones de internet constituido en forma de persona jurídica, el que deberá mantener los respectivos registros de acceso a aplicaciones de internet, en secreto, en ambiente controlado y de seguridad, por el plazo de seis meses, en los términos de los artículos 13, 14, 15 y 16 del reglamento.

Mención a la confidencialidad en la LGPD, consta en el artículo 5 que determina el glosario de términos, por el cual los datos personales confidenciales son aquellos sensibles, esto es, datos sobre origen racial o étnico, convicción religiosa, opinión política, afiliación sindical u organización religiosa, filosófica o política, datos de salud o vida sexual, datos genéticos o biométricos, cuando están vinculados a una persona natural.

Otra mención sobre confidencialidad se encuentra en el Capítulo VII sobre Seguridad y buenas prácticas, en la sección I, denominada Seguridad y confidencialidad de datos. En la cual, se analizaron todos los mecanismos técnicos y administrativos que permiten el resguardo de la información. De esta manera, se concluye que no consta en la normativa

brasileña alusión al derecho a la confidencialidad sino que esta se entiende desarrollado a través del principio de seguridad de los datos personales.

ix. Derecho al olvido digital

No existe referencia normativa al respecto.

x. Spam

El artículo 5 del Reglamento a la Ley Marco Civil de Internet hace alusión al *spam* cuando señala que para la prestación adecuada de servicios y aplicaciones por parte del responsable de actividades de transmisión, de conmutación o de enrutamiento, en el marco de su respectiva red, y que tienen como objetivo mantener su estabilidad, seguridad, integridad y funcionalidad, será requisito técnico indispensable el tratamiento de cuestiones de seguridad de redes, tales como restricción al envío de mensajes masivos (*spam*) y control de ataques de denegación de servicio.

xi. Limitación al tratamiento:

El artículo 6 de la LGPD señala el principio de necesidad por el cual se limita "el tratamiento al mínimo necesario para la realización de sus fines, con cobertura de los datos pertinentes, proporcionados y no excesivos en relación con los fines del tratamiento de datos". Es decir se atiende a una limitación en la captación de la data para lo cual es necesario identificar la finalidad del tratamiento con lo cual se puede determinar los datos pertinentes y necesarios para un tratamiento adecuado.

Este principio es de difícil comprensión y aplicación en el caso del *big data* y por ello suele ser ampliamente controvertido, toda vez que, este procesamiento es uno de aquellos que permite la creación de perfiles de cualquier tipo; y, por ende, puede generar mayores riesgos a los titulares de los datos personales.

Asimismo, el numeral II del artículo 16 el Marco Civil de Internet se reformó a través de la LGPD puesto que ahora señala que, si bien, en la provisión de conexión, onerosa o gratuita, está prohibida la custodia de aquellos datos personales que son excesivos en relación con el propósito para el cual su propietario dio su consentimiento, ahora se admite las excepciones previstos en la Ley de protección de datos personales.

xii. Portabilidad

El artículo 18 número V menciona como derecho de los titulares a la portabilidad de los datos a otro proveedor de servicios o productos. Por la forma de redacción de la norma, se entiende que el concepto de portabilidad es equivalente a comunicación o entrega de datos entre proveedores. Con ello se soluciona la distinción que existe entre portabilidad de datos, de buscadores y de redes sociales, pues se asume que opera en todas estas. No existe diferenciación entre datos entregados por el propio titular, de aquellos entregados por tercero. Tampoco se menciona el formato, la obligación de eliminación o la posibilidad de replicar o copiar. Únicamente se establece que, será la autoridad nacional la que a través de reglamentos determine las característicasa de los mecanismos de transferencia, en especial de aquellos temas relativos a secretos comerciales e industriales.

La norma se limita a señalar que la portabilidad debe ser solicitada de forma previa y expresa.

xiii. Confirmación de la existencia de tratamiento

El artículo 18 número I señala que el titular tiene derecho a confirmar la existencia de tratamiento. Esta precisión realizada por el legislador podría está contenida en el derecho de acceso. Sin embargo, el haberlo establecido de forma expresa y diferenciada se pretende que en su disponibilización se pueda agilitar la defensa de los derechos del titular.

xiv. Comunicación de datos entre públicos

En el artículo 18 número VII se determina el derecho de los titulares de ser informados sobre entidades públicas y privadas con las cuales el controlador hizo uso compartido de datos. Este derecho atiende a la necesidad de que la ciudadanía confíe en el estado como responsable de tratamiento porque lo obliga a informar al titular sobre las comunicaciones de sus datos que se realicen entre instituciones públicas. De esta forma el ciudadano queda advertido y de ser necesario puede ejercitar los otros derechos previamente analizados.

g. Procedimiento

El Marco Civil de Internet, en el artículo 30, señala que la defensa de los intereses y derechos establecidos en esta ley podrá ser ejercida individual o colectivamente. Conforme el artículo 21 del Reglamento, respecto de las infracciones descritas en la Ley Marco Civil de Internet y en el mismo reglamento, se podrán iniciar las acciones de oficio o mediante requerimiento de cualquier interesado y serán aplicables los procedimientos internos de cada uno de los órganos fiscalizatorios: a) Anatel en Telecomunicaciones; b) Secretaría Nacional del Consumidor respecto a derechos del consumidor; c) Sistema Brasileño de Defensa de la Competencia; y d) Comité Gestor de Internet en Brasil, CGIbr, y las entidades de la administración pública federal.

El Reglamento de la Ley citada, en el artículo 11, señala un procedimiento específico que deben seguir las autoridades administrativas competentes autorizadas por ley, conforme el artículo 10, § 3º de la Ley 12.965, de 2014, para la solicitud de datos catastrales.

Por su parte, el artículo 13 del mismo reglamento, respecto de proveedores de conexión y de aplicación que custodian, almacenan o tratan datos personales y comunicaciones privadas, establecen la obligación de crear un inventario detallado de los accesos a los registros de conexión y de acceso a aplicaciones, conteniendo el momento, la duración, la identidad del funcionario o del responsable del acceso designado por la empresa y el archivo accedido. Este registro permite que se dé cumplimiento de lo dispuesto en el artículo 11, § 3º, de la Ley 12.965, de 2014. Dicho de otro modo, los proveedores de conexión y de aplicaciones de internet deberán presentar, en línea con la reglamentación, información que permita la verificación del cumplimiento de la legislación brasileña en lo referente a la recolección, protección, almacenamiento o tratamiento de datos, así como en lo que respecta a la privacidad y al secreto de las comunicaciones.

En cuanto a los procedimiento previstos en la LGPD se estará a lo dispuesto en el numeral 3º del artículo 18 de la LGPD que establece que todos los derechos enunciados en esta norma[1182] serán ejercidos a requerimiento expreso del titular o de representante legalmente constituido directamente al agente de tratamiento.

Ahora bien, el numeral V, del artículo 55 de la LGPD determina que la Autoridad Nacional de Protección de Datos es responsable de considerar las peticiones del titular cuando el controlador no ha resuelto dentro del período establecido por la regulación la queja presentada por el titular. En tal sentido, la Autoridad Nacional además de resolver sobre el derecho del titular podrá investigar, multar y aplicar sanciones al controlador, por incumplimiento de la ley.

Estas quejas, deberán recolectarse y analizarse en forma agregada, y cualquier medida resultante de ellas puede adoptarse de manera estandarizada, al tenor de lo señalado en el Párrafo 6 de la norma citada.

Así mismo, el citado artículo 55 en el numeral XXIV, señala entre las responsabilidad de la Autoridad Nacional, la de implementar mecanismos simplificados, incluso por medios electrónicos, para el registro de quejas sobre el procesamiento de datos personales en incumplimiento de esta Ley. En este caso, el procedimiento de denuncia es directo sin que se exija su presentación previa al agente del tratamiento.

Adicionalmente, conforme dispone el artículo 22 de la LGPD la defensa de los intereses y de los derechos de los titulares de datos podrán ser ejercidos en juicio, de forma individual o colectiva. Para lo cual el titular deberá acogerse a lo señalado en la legislación pertinente, acerca de los instrumentos de tutela individual y colectiva.

Como vemos, los mecanismos de tutela para la protección de datos personales son amplios, pues incluyen acciones administrativas que se ejercen directamente ante el agente de tratamiento; así como de revisión en caso de no respuesta por parte del responsable de tratamiento; e incluso de denuncia directa, a través de medios electrónicos, sin necesidad de agotamiento de vía, es decir que no hayan sido previamente puestos en conocimiento ante el agente de tratamiento.

[1182] "Artículo 18. El titular de los datos personales tiene derecho a obtener del controlador, en relación con los datos del titular procesados por él, en cualquier momento y previa solicitud:
I - confirmación de la existencia de tratamiento;
II - acceso a los datos;
III- corrección de datos incompletos, inexactos u obsoletos;
IV- anonimato, bloqueo o eliminación de datos innecesarios, excesivos o tratados en violación de las disposiciones de esta Ley;
V- portabilidad de los datos a otro proveedor de servicios o productos, previa solicitud expresa, de conformidad con los reglamentos de la autoridad nacional, sujeto a secretos comerciales e industriales;
VI- eliminación de datos personales procesados con el consentimiento del titular, excepto en los casos previstos en el art. 16 de esta Ley;
VII- información sobre entidades públicas y privadas con las cuales el controlador hizo uso compartido de datos;
VIII- información sobre la posibilidad de no dar consentimiento y sobre las consecuencias del rechazo;
IX - revocación del consentimiento, de conformidad con el § 5 del art. 8 de esta Ley […]"

Asimismo, existen otros mecanismos judiciales de carácter constitucional y legal en ámbitos civiles y penales todo a cuenta de diferenciar los distintos niveles de gravedad y por ende, de responsabilidad que pudieran atribuirse a los inadecuados tratamientos de datos personales que pudieran suscitarse.

g) Habeas data

i. Legitimado activo

La Constitución brasileña determina que serán sujetos activos del *habeas data* las personas naturales brasileñas y extranjeras residentes en el país, de conformidad con lo señalado en el artículo 5 de esta Carta Magna.[1183]

ii. Legitimado pasivos u obligados

De acuerdo con lo señalado en el artículo 5 de la norma constitucional brasileña, el *habeas data* solo tiene como sujeto pasivo a las entidades gubernamentales o de carácter público que almacenan datos catastrales. Esto porque esta norma constitucional no ha sido modificada y en consecuencia no se integran aún a la esfera de protección del *habeas data*, las bases privadas.

iii. Derechos tutelados por el habeas data

No existe alusión a los derechos que son tutelados mediante el *habeas data*, pero por la simple lectura del artículo 5 de la Constitución se infiere que protege a la autodeterminación informativa. Ya que, conforme señala el citado artículo se concederá *habeas data* para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público y para la rectificación de datos.

iv. Procedencia del habeas data

La procedencia del *habeas data* no está determinada en la normativa constitucional ni legal; sin embargo, de la lectura de la norma constitucional se colige que se concederá *habeas data* cuando los datos personales se encuentren en registros o bancos de datos de entidades gubernamentales o de carácter público y cuando lo que se pretenda sea la rectificación de los datos.[1184]

v. Procedimiento del habeas data

En el artículo 5 LXXII se reconoce tanto el derecho de información como el de rectificación, y en el LXXVII se aclara la gratuidad de las acciones constitucionales, además de la mención expresa de otras vías de reclamo como la secreta, la judicial o la administrativa. El mandato de seguridad no es procedente cuando el derecho está amparado por el *habeas data* conforme lo dispone el artículo 5, apartado LXIX de la Constitución.

[1183] Brasil, *Constitución de 1988*, accedido 22 de mayo de 2017, http://pdba.georgetown.edu/Constitutions/Brazil/esp88.html.
[1184] Ibíd.

El *habeas data* establece un sistema procesal que permite su eficacia plena, pues en los artículos 102,[1185] 105,[1186] 108[1187] y 109[1188] de la Constitución Política de la República Federativa de Brasil de 1988 se desarrolla la competencia, tanto del Supremo Tribunal Federal del Brasil, del Tribunal Superior de Justicia, de Tribunal Regional Federal, como de los jueces federales de conocer sobre el *habeas data,* categorizando además los casos de fuero.

h) Institucionalidad de protección

Con base en lo dispuesto en el artículo 20 del Marco Civil de Internet, los órganos y las entidades de la administración pública federal con competencias específicas acerca de los asuntos relacionados con este Decreto, actuarán de forma colaborativa, para lo cual considerarán las directrices emitidas por el Comité Gestor de Internet en Brasil o sus siglas CGIbr.[1189] En colaboración, deberán velar por el cumplimiento de la legislación brasileña, inclusive respecto de la aplicación de las sanciones cabales aunque las actividades sean realizadas por una persona jurídica con sede en el exterior, de conformidad con el artículo de la Ley 12.965, de 2014.

Conforme el artículo 13, § 10 del Reglamento de Marco Civil de Internet, corresponde al CGIbr promover estudios y recomendar procedimientos, normas y estándares técnicos y operativos para garantizar la seguridad de los datos personales almacenados y tratados, de acuerdo con las especificidades y el porte de los proveedores de conexión y de aplicación.

Respecto de la institucionalidad encargada de la protección de datos personales en el Brasil, la LGPD, señala como órgano competente a la Autoridad Nacional de Protección de Datos Personales.

La configuración de esta entidad ha tenido varios tropiezos. La versión original de la Ley de Protección de Datos Personales, LGPD, 13,709/18[1190], fue dictada en agosto de 2018 y si bien fue aprobada por unanimidad en la Cámara y en el Senado, fue vetada en lo relativo a la institucionalidad, por el Presidente Michael Temer. Quien, para diciembre del mismo año, dicta una Orden Ejecutiva denominada Medida Provisoria

[1185] "Artículo 102. Compete al Supremo Tribunal Federal, principalmente, la guarda de la Constitución, cabiéndole: I. Procesar y juzgar, originariamente: [...] d) el *hábeas corpus*, siendo paciente cualquiera de las personas referidas en los párrafos anteriores; el mandato de *segurança* y el *hábeas data* contra actos del presidente de la República, de las Mesas de la Cámara de Diputados y del Senado Federal, del Tribunal de Cuentas de la Unión, del procurador general de la República y del propio Supremo Tribunal Federal. II. Juzgar, en recurso ordinario: *a*) el *hábeas corpus*, el mandato de *segurança*, el *hábeas data* y el mandato de *injuncao* decididos en única instancia por los Tribunales Superiores, si la decisión fuere denegatoria." Ibíd.

[1186] "Art. 105. Compete al Tribunal Superior de Justicia: I. Procesar y juzgar, originariamente: [...] *b*) los mandatos de *segurança*, los *hábeas data* contra acto de Ministro de Estado o del propio Tribunal." Ibíd.

[1187] "Art. 108. Compete a los Tribunales Regionales Federales: I. Procesar y juzgar, originariamente: [...] *c*) los mandatos de *segurança* y los *hábeas data* contra acto del propio Tribunal o de juez federal." Ibíd.

[1188] "Art. 109. A los jueces federales compete procesar y juzgar: [...] VIII. Los mandatos de *segurança* y los *hábeas data* contra acto de autoridad federal, exceptuados los casos de competencia de los tribunales federales." Ibíd.

[1189] NIC.BR, *Decreto4.829*, de 3 /09/ 003 que crea el CGI.br - Comitê Gestor da Internet no Brasil", *CGI.br - Comitê Gestor da Internet no Brasil*, accedido 26 de mayo de 2017, http://cgi.br.

[1190] Brasil, Ley N ° 13.709, de 14 de agosto de 2018, accedido el 20 de agosto de 2018, http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

No. 869/18[1191], en la que si bien crea la Autoridad Nacional Brasileña de Protección de Datos, ANPD, le otorga naturaleza transitoria, pues al cabo de dos años, deberá ser evaluada y a discreción del gobierno, podrá transformarse en una autarquía vinculada a la Presidencia de la República.[1192]

Para el 9 de julio de 2019, se publica la Ley 13.853/19[1193] que acoge los criterios dispuestos en la Medida Provisoria No. 869/18, modifica la Ley LGPD, 13,709/18, y además incorpora los nueve vetos dispuestos por el actual presidente del Brasil, Jair Bolsonaro. Uno de los vetos prohibió a la ANPD cobrar honorarios por los servicios prestados, por lo que la principal fuente de financiamiento del órgano de control será el Presupuesto de la Unión, junto con otras relativas a donaciones o comodatos. Situación que puede afectar una de las formas de independencia básica de este tipo de entidades que es la financiera y presupuestaria.[1194]

La citada LGPD, en su artículo 55-A, crea la Autoridad Nacional de Protección de Datos, en adelante ANPD, como organismo de administración pública federal miembro de la Presidencia de la República. Esta dependencia se justifica en la necesidad de no incrementar gastos estatales. Y se manifiesta también en el artículo 55-G. de la LGPD que señala al Presidente de la República como autoridad responsable de dictar la estructura organizacional y funcional de la entidad; además, de atribuir los recursos que requerirán de autorización expresa física y financiera en la ley de presupuesto anual. Pero sobre todo, la máxima autoridad del Poder Ejecutivo, designará a los miembros del Consejo Directivo, previa aprobación del Senado Federal. Ahora bien, al menos en el texto de ley, consta reconocida la autonomía técnica y de toma de decisiones de la ANPD, artículo 55B.

El artículo 55C de la LGPD determina la conformación de la ANPD de la siguiente forma:

a) Junta Directiva: es el máximo órgano de gobierno y está compuesto por cinco directores, incluido el CEO, artículo 55D Serán brasileños de reputación intachable, nivel superior de educación y un alto grado en el campo de especialidad. Nombrados por un lapso de 4 años.

a) Consejo Nacional de Protección de Datos Personales y Privacidad: Será responsable de proponer estrategias y subsidios para la elaboración de la Política nacional de protección de datos personales y privacidad y para el desempeño de la ANPD; así como evaluar las acciones de la citada Política; sugerir acciones; preparar estudios, celebrar debates públicos y audiencias; y difundir conocimientos sobre la temática, al tenor del artículo

[1191] Brasil, Medida Provisional 869/18, accedido el 20 de agosto de 2019, http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/57220361/do1-2018-12-28-medida-provisoria-n-869-de-27-de-dezembro-de-2018-57219992

[1192] "Se sanciona una ley que crea la Autoridad Nacional de Protección de Datos", E-Health Reporter Latinoamérica, accedido el 22 de agosto de 2019, en https://ehealthreporter.com/es/noticia/se-sanciona-una-ley-que-crea-la-autoridad-nacional-de-proteccion-de-datos/

[1193] Brasil, Ley N ° 13.853 del 8 de julio de 2019, accedido el 20 de agosto de 2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1

[1194] "Se sanciona una ley que crea la Autoridad Nacional de Protección de Datos", E-Health Reporter Latinoamérica, accedido el 22 de agosto de 2019, en https://ehealthreporter.com/es/noticia/se-sanciona-una-ley-que-crea-la-autoridad-nacional-de-proteccion-de-datos/

58B. Estará compuesto por 23 representantes, titulares y suplentes, de los siguientes organismos: cinco del Poder Ejecutivo federal (nombrados por el Presidente); uno del Senado Federal; uno de la Cámara de Diputados; uno del Consejo Nacional de Justicia; uno del Consejo Nacional del Ministerio Público; uno del Comité Directivo de Internet de Brasil; tres de las entidades de la sociedad civil relacionadas con la protección de datos personales; tres de instituciones científicas, tecnológicas y de innovación; tres de las confederaciones sindicales que representan categorías económicas del sector productivo; dos de las entidades que representan al sector empresarial relacionado con el procesamiento de datos personales; y dos de entidades que representan al sector laboral. Nombrados por un lapso de 2 años, con una renovación permitida. La participación en este Consejo se considera prestación de servicio público relevante y no será remunerada, artículo 58A de la LGPD. La forma de conformación de este Consejo, tal como vemos, nuevamente tiene una alta representación del ejecutivo. Ahora bien, es referente en la región el establecimiento de este tipo de órganos de amplia representación que tiene una responsabilidad de evaluación y consulta de las actividades llevadas a cabo por la ANPD.

c) Asuntos internos;
d) Defensor del Pueblo;
e) organismo asesor jurídico propio; y
f) unidades administrativas y unidades especializadas necesarias para la aplicación de las disposiciones de esta Ley.

El artículo 55J de la LGPD establece las responsabilidades de la ANPD, entre las más importantes constan las siguientes:

a) garantizar la protección de datos personales;
b) elaborar directrices para la Política nacional de protección de datos personales y privacidad;
c) supervisar y aplicar sanciones en caso de incumplimientos de la Ley;
d) resolver las peticiones del titular no satisfechas por los agentes de tratamiento;
e) promover y capacitar a la ciudadanía, así como elaborar investigaciones sobre el derecho a la protección de datos personales;
f) promover acciones de cooperación con otras autoridades nacionales, internacionales o transnacionales;
g) solicitar a las autoridades públicas que lleven a cabo operaciones de procesamiento de datos personales proporcionar información sobre los procesamientos realizados, y emitir, de ser el caso, opinión técnica para garantizar cumplimiento de esta ley;
h) dictar reglamentos y procedimientos, así como sobre informes de impacto en la protección de datos personales para casos en los que el tratamiento representa un riesgo elevado para garantizar los derechos y principios;
i) editar reglas, pautas y procedimientos simplificados y diferenciados, incluidos los plazos, para que las micro y pequeñas empresas, así como las iniciativas comerciales incrementales o disruptivas que se autodenominan *startups* o compañías de innovación, puedan adaptarse a esta Ley; entre otros.

Es destacable en esta normativa, que las regulaciones y reglas emitidas por la ANPD tendrán un proceso de formación precedido de consultas y audiencias públicas, así como de análisis de impacto regulatorio.

La Ley entrará en vigor a partir de agosto de 2020. Hasta entonces, la ANPD deberá estructurarse incluido el nombramiento de sus autoridades y el decreto que lo habilita.

i) Régimen sancionador

El artículo 12 de la Ley de Marco Civil de Internet deja constancia de que las actuaciones indebidas de los responsables de transmisión, conmutación o ruteo de tratar, de la custodia y entrega de los registros de conexión y de acceso a aplicaciones de internet de que trata esta ley, así como de los datos personales y del contenido de las comunicaciones privadas tendrán responsabilidad civil, penal y administrativa. Además, establece una serie de infracciones a las normas previstas en los artículos 10 y 11 del mismo cuerpo legal instaurando como sanciones aplicadas de forma individual o acumulativa las siguientes: I – advertencia, con indicación de plazo para la adopción de medidas correctivas; II – multa de hasta el 10% (diez por ciento) de lo facturado por el grupo económico en Brasil en su último ejercicio, excluidos los impuestos, considerando la condición económica del infractor y el principio de proporcionalidad entre la gravedad de la falta y la gravedad de la sanción; III – suspensión temporal de las actividades que involucren los actos previstos en el artículo 11; o IV – prohibición de ejercicio de las actividades que involucren los actos previstos en el artículo 11. *Párrafo único.* Cuando se trate de una empresa extranjera, responde solidariamente del pago de la multa de que trata este artículo su filial, sucursal, oficina o establecimiento situado en el país.

Finalmente, el Reglamento de Marco Civil de Internet establece en los artículos 17, 18, 19, 20 y 21, los entes responsables de verificar el cumplimiento, tanto de la Ley como del mismo Reglamento. Cada uno de ellos en los ámbitos de aplicación de la normativa que le corresponde. Esto, por cuanto Anatel actuará en la regulación, fiscalización y recuento de infracciones, en los términos de la Ley 9.472, 16 de julio de 1997, Ley General de Telecomunicaciones 9.472 (art. 17).

La Secretaría Nacional del Consumidor actuará en la fiscalización y recuento de infracciones, en los términos de la Ley 8.078, 11 de septiembre de 1990, ley que dispone sobre la protección al consumidor y dicta otras providencias (art. 18).

El recuento de infracciones al orden económico quedará a cargo del Sistema Brasileño de Defensa de la Competencia que, en los términos de la Ley n.° 12.529, 30 de noviembre de 2011, de Estructura del Sistema Brasileño de Defensa de la Competencia, establece sobre la prevención y represión de las infracciones contra el orden económico (art. 19).

Como se vio en el ítem anterior, el artículo 20 del Reglamento determina que los órganos y las entidades de la administración pública federal sobre asuntos relacionados con el Marco Civil de Internet su Ley y Reglamento, tomarán en cuenta las directrices del Comité Gestor de Internet en Brasil.

> Finalmente, el artículo 21 señala que respecto de las infracciones a la Ley Marco Civil de Internet, se atenderá a los procedimientos internos de cada uno de los órganos fiscalizatorios antes citados y podrá ser iniciada de oficio o mediante requerimiento de cualquier interesado.

Por su parte, el Capítulo VIII Supervisión, en la Sección I denominada de las sanciones administrativas de la LGPD el artículo 52 señala que, si agentes de tratamiento de datos incurrierran en algunas de las infracciones descritas en la citada normativa, podrán ser sancionados por la autoridad nacional a través de los siguientes mecanismos: advertencia, con indicación de plazo para la adopción de medidas correctivas; multa simple, de hasta el 2% (dos por ciento) de la facturación de la persona jurídica de derecho privado, grupo o conglomerado en Brasil en su último ejercicio, excluidos los tributos, limitada, en total, a R $ 50.000.000,00 (cincuenta millones de reales) por infracción; multa diaria, observado el límite total previamente previsto; publicidad de la infracción; bloqueo de los datos personales a que se refiere la infracción hasta su regularización; o eliminación de los datos personales a que se refiere la infracción.

Fueron vetadas por el Presidente tres mecanismos sancionatorios adicionales aprobados por el Congreso, los numerales X[1195], XI[1196] y XII[1197] relativos a suspensiones o prohibiciones de procesamiento de datos o del ejercicio de la actividad relacionada con el procesamiento de dato. El Presidente señaló como fundamento de su veto que estas sanciones administrativas crean:

> […] inseguridad para los responsables de esta información, así como también impide el uso y procesamiento de bases de datos esenciales para diversas actividades privadas. , como los utilizados por las instituciones financieras, que podrían dañar la estabilidad del sistema financiero nacional, así como las entidades públicas, con el potencial de afectar la continuidad de los servicios públicos.[1198]

Lo que queda claro es que, cualquier sanción deberá imponerse luego del procedimiento administrativo que permite la oportunidad de defensa legal.

Además la imposición de la sanción deberá tomar en cuenta la gravedad y la naturaleza de las infracciones y de los derechos personales afectados; la buena fe del infractor; la ventaja obtenida o pretendida por el infractor; la condición económica del infractor; la reincidencia; el grado del daño; la cooperación del infractor; la adopción repetida de mecanismos internos y procedimientos que reduzcan al mínimo el daño; la adopción de

---

[1195] Brasil, Ley N ° 13.853 del 8 de julio de 2019, accedido el 20 de agosto de 2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1 ,"Artículo 52 numeral X: suspensión parcial de la operación de la base de datos a la que se refiere la infracción por un período máximo de 6 (seis) meses, prorrogable por el mismo período, hasta que el controlador haya regularizado la actividad de tratamiento",

[1196] Brasil, Ley N ° 13.853 del 8 de julio de 2019, accedido el 20 de agosto de 2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1 ,"Artículo 52 numeral XI: suspensión del ejercicio de la actividad de la base de datos ; procesamiento de datos personales a los que se refiere la infracción por un período máximo de seis (6) meses, prorrogable por el mismo período,

[1197] Brasil, Ley N ° 13.853 del 8 de julio de 2019, accedido el 20 de agosto de 2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1 , "Artículo 52 numeral XII - prohibición parcial o total del ejercicio de actividades de procesamiento de datos"

[1198] Brasil, Ley N ° 13.853 del 8 de julio de 2019, accedido el 20 de agosto de 2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1

políticas de buenas prácticas y gobernanza o de pronta adopción de medidas correctivas; y la proporcionalidad entre la gravedad de la falta y la intensidad de la sanción.

Las disposiciones de este artículo no sustituyen la aplicación de penal administrativa, civil o aquella propia de alguna legislación específica.

Finalmente, se recalca el proceso colaborativo de elaboración del reglamento sobre sanciones administrativas a infracciones a esta Ley, que tiene por objeto definir la metodología que orientará el cálculo del valor base de las sanciones de multa; las circunstancias y condiciones para la adopción de una multa simple o diaria; los criterios de gravedad de la falta y extensión del daño, entre otros. Pues para su aprobación deberá realizarse un proceso de consulta pública, al tenor de los artículos 53 y 54 de la LGPD.

j) Transferencia internacional de datos

La Ley de Marco Civil señala en el artículo 11 que cualquier operación de recolección, almacenamiento, protección o tratamiento de datos personales o de comunicaciones por proveedores de conexión y aplicaciones de Internet, debe respetar la legislación brasileña. En suma, dicha normativa no establece referencia alguna a las transferencias internacionales de datos personales, tanto más que aclara que solo es aplicable a datos recolectados en territorio nacional y al contenido de las comunicaciones en que al menos uno de los terminales está localizado en Brasil, o que oferten servicios al público brasileño o que al menos una integrante del mismo grupo económico posea un establecimiento en Brasil.

La transferencia internacional de datos personales realmente ha sido regulada en la LGPD a través del Capítulo V denominado Transferencia de datos de la internacional, que en su artículo 33 señala que sólo está permitida en los siguientes casos:

a) *Países adecuados:* para países u organismos internacionales que proporcionen grado de protección de datos personales adecuado a lo previsto en esta Ley. Conforme señala el artículo 34 de la LGPD, el nivel de protección será evaluado por la autoridad nacional, bajo las siguientes consideraciones: normas generales y sectoriales de la legislación vigente en el país de destino o en el organismo internacional; naturaleza de los datos; observancia de los principios generales; adopción de medidas de seguridad; existencia de garantías judiciales e institucionales; y otras circunstancias específicas.

b) *Garantías de cumplimiento:* cuando el controlador ofrezca y comprobará garantías de cumplimiento de los principios, de los derechos del titular y del régimen de protección de datos, en la forma de cláusulas contractuales específicas para una determinada transferencia; cláusulas estándar contractuales; normas corporativas globales; sellos, certificados y códigos de conducta regularmente expedidos. En este sentido, el artículo 35 de la LGPD señala que la definición del contenido de estos mecanismos será realizado por la autoridad nacional, para lo cual se considerarán los requisitos, condiciones y garantías mínimas, los derechos, garantías y principios previstos en la LGPD. Para la verificación de las operaciones de tratamiento, se podrá requerir informaciones suplementarias. Asimismo, las alteraciones en las garantías suficientes deberán

comunicarse a la autoridad nacional, conforme el artículo 36 de la LGPD. La ANPD podrá autorizar organismos de certificación para autorizar el contenido y seguimiento de estos mecanismos de garantía de protección, bajo su supervisión.

c) *Cooperación jurídica internacional:* cuando la transferencia sea necesaria entre los organismos de inteligencia pública, investigación y enjuiciamiento, de conformidad con los instrumentos del derecho internacional.
d) *Protección a la vida e integridad*: cuando la transferencia es necesaria para proteger la vida o la seguridad física del titular o de un tercero.
e) *Autorización expresa:* cuando la autoridad nacional autoriza la transferencia.
f) *Acuerdo de cooperación internacional:* cuando la transferencia resulta en un compromiso hecho en un acuerdo de cooperación internacional.
g) *Ejecución de competencias públicas:* cuando la transferencia sea necesaria para la política pública de ejecución o autoridad legal de servicio público.
h) *Consentimiento del titular específico:* cuando el titular ha dado su consentimiento específico, previamente informado de la operación internacional.
i) Cumplimiento de una obligación legal, contractual y ejercicio de derechos en procesos judiciales y arbitrales.

k) Delegado de protección de datos: Responsable

El artículo 5 de la LGPD en sus definiciones señala que el responsable será la persona designada por el controlador y el operador para que actúe como un canal de comunicación entre el controlador, los interesados y la ANPD.

Resulta interesante esta propuesta, puesto que la principal función asignada es la de ser un enlace, al parecer un mediador canalizador de necesidades e inquietudes entre agentes de tratamiento, titulares de datos y autoridad de control. Las referencias sobre el delegado en el RGPD suelen ir dirigidas a su carácter supervisor o controlador de las actividades del responsable, rol que en este caso no se encuentra claramente determinado.

Ahora bien, el artículo 41 de la LGPD señala que el controlador será quien designe al responsable. Adicionalmente, esta norma señala que la identidad de esta persona y su información de contacto se divulgarán de manera pública, clara y objetiva, preferiblemente en el sitio web del controlador, esto con la intención de que los titulares de los datos puedan satisfacer de forma inmediata sus requerimientos o recibir al apoyo para el ejercicio de sus derechos.

Entre sus responsabilidades estará las de aceptar quejas y comunicaciones de los titulares, proporcionar aclaraciones y adoptar medidas; recibir comunicaciones de la autoridad nacional y adoptar medidas; asesorar a los empleados y contratistas de la entidad con respecto a las prácticas que se tomarán en relación con la protección de datos personales; y realizar informes sobre el impacto de la protección de datos personales. Estas actividades asignadas reflejan el rol coordinador más que controlador de su designación, por lo que lejos de ser un brazo preventorio o ejecutor de la ANPD, será un trabajador al servicio de la entidad tratante de datos.

Adicionalmente, la ANDP podrá establecer reglas complementarias sobre sus atribuciones, incluida la posibilidad de que debido a la naturaleza y el tamaño de la

entidad o el volumen de las operaciones de procesamiento de datos se pueda exonerar de la necesidad de su nombramiento.

Finalmente, en la versión anterior al veto constaba un apartado 4 del artículo 41 que determinaba que el responsable debía ser una persona con conocimientos legales y reglamentarios especializados sobre protección de datos. Además que cargo o cargos dentro de un grupo empresarial tiene, y la mención expresa de su autonomía técnica y profesional en la oficina.

El Presidente argumentó en su veto que este texto:

> […] contradice el interés público, ya que es un requisito con un rigor excesivo que se refleja en la interferencia innecesaria del Estado a la discreción de seleccionar cuadros del sector productivo, además de vulnerar el derecho fundamental, previsto en el artículo 5, XIII de la Constitución, al restringir el ejercicio profesional gratuito hasta el punto de alcanzar su núcleo esencial.

El veto fue a la totalidad del texto, lo que resulta contradictorio, pues la argumentación corresponde únicamente a la profesión o conocimientos del responsable, cuando el artículo vetado en su totalidad hace alusión a la independencia que requiere esta persona para el ejercicio de sus funciones. Características que no debieron ser eliminadas del texto de la ley, debido a la necesidad de transparencia e imparcialidad en el ejercicio de las competencias asignadas.

2.3 Colombia (1991)

Colombia en su Constitución de 1991,[1199] en el Título II relativo a los derechos, las garantías y los deberes, en el capítulo 1, "De los Derechos Fundamentales" en el artículo 15 consagró un derecho al control de la información del individuo cuyo texto expresamente señala:

> Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.[1200]

La Corte Constitucional, respecto del alcance de esta norma, señala que:

> En efecto, el artículo 15 de la Carta reconoce tres derechos: (i) el derecho a la intimidad, (ii) el derecho al buen nombre y (iii) el derecho al *habeas data*. La Sala observa que si bien el derecho al *habeas data* está estrechamente ligado con los derechos a la intimidad y al buen nombre, todos los anteriores son derechos con contenidos autónomos y diferentes...

[1199] Modificada en 1993, 1995, 1996, 1997, 1999, 2000, 2001, 2002, 2003, 2004, 2005 y 2009.
[1200] Colombia, Asamblea Nacional Constituyente, "Colombia: Constitución de 1991 con reformas hasta 2009", *Political Database of the Americas*, 1991, accedido 29 de junio de 2017, http://pdba.georgetown.edu/Constitutions/Colombia/vigente.html.

Asimismo, en la misma Constitución colombiana de 1991, en el capítulo 4, "De la Protección y Aplicación de los Derechos", consagra la figura constitucional de la acción de tutela, concibiéndola como una garantía constitucional la protección de los datos personales. El texto del artículo 86 de la Carta Política colombiana dice:

> Artículo 86. Toda persona tendrá acción de tutela para reclamar ante los jueces, en todo momento y lugar, mediante un procedimiento preferente y sumario, por sí misma o por quien actúe a su nombre, la protección inmediata de sus derechos constitucionales fundamentales, cuando quiera que éstos resulten vulnerados o amenazados por la acción o la omisión de cualquier autoridad pública.
> La protección consistirá en una orden para que aquél respecto de quien se solicita la tutela, actúe o se abstenga de hacerlo. El fallo, que será de inmediato cumplimiento, podrá impugnarse ante el juez competente y, en todo caso, éste lo remitirá a la Corte Constitucional para su eventual revisión.
> Esta acción sólo procederá cuando el afectado no disponga de otro medio de defensa judicial, salvo que aquella se utilice como mecanismo transitorio para evitar un perjuicio irremediable.
> En ningún caso podrán transcurrir más de diez días entre la solicitud de tutela y su resolución.
> La ley establecerá los casos en los que la acción de tutela procede Contra particulares encargados de la prestación de un servicio público o cuya conducta afecte grave y directamente el interés colectivo, o respecto de quienes el solicitante se halle en estado de subordinación o indefensión.

Posteriormente, se promulgó la Ley 1266 de *Habeas Data* de 2008,[1201] que regula el manejo de la información personal contenida en bases financieras, crediticias, comerciales, de servicios y la proveniente de terceros países. "No obstante, al analizar el contenido de la norma se observa que se encuentra orientada a la protección de los datos comerciales y financieros y deja vacíos normativos en orden a garantizar su completa protección en Colombia"[1202].

Para desarrollar la Ley en mención existen dos decretos reglamentarios:

a) Decreto 1727 de 2009, por el cual se determina la forma en la que los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la misma, publicado en el Diario Oficial 47.350, 15 de mayo de 2009.[1203]

b) Decreto 2952 de 2010, por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008, publicado en el Diario Oficial 47.793, 6 de agosto de 2010.[1204]

En la jurisprudencia constitucional colombiana se aclara las líneas interpretativas por las cuales paulatinamente el *habeas data* ha adquirido un contenido esencial propio que le

[1201] Senado de la República, "Ley hábeas data y manejo de la información contenida en bases de datos personales (Ley 1266 de 2008) - vLex Global".
[1202] M. R. BEJARANO, "Evolución del Derecho de Protección de Datos Personales en Colombia respecto a estándares internacionales", *Novum Jus: Revista Especializada en Sociología Jurídica y Política*, vol. 8, 1, 2014, accedido 26 de mayo de 2017, http://editorial.ucatolica.edu.co/ojsucatolica/revistas_ucatolica/index.php/Juridica/article/view/652.
[1203] Colombia, Presidencia de la República de Colombia, *Decreto 1727* de 2009, por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial...".
[1204] Colombia, Presidencia de la República de Colombia, "Decreto 2952 de 2010, por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008".

permite constituirse como un derecho fundamental, independiente y autónomo de la intimidad y del libre desarrollo de la personalidad.

> [...] el derecho al *habeas data* fue primero interpretado como una garantía del derecho a la intimidad, de allí que se hablara de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir. También, desde los primeros años de la nueva Carta, surgió al interior de la Corte una segunda línea interpretativa que consideraba el *habeas data* una manifestación del libre desarrollo de la personalidad. Según esta línea, el *habeas data* tiene su fundamento último "(...) en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad. Ya a partir de 1995, surge una tercera línea interpretativa que es la que ha prevalecido desde entonces y que apunta al *habeas data* como un derecho autónomo, en que el núcleo del derecho al *habeas data* está compuesto por la autodeterminación informática y la libertad – incluida la libertad económica. Este derecho como fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben pender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones"[1205].

Sobre la naturaleza autónoma de los derechos fundamentales del titular, de los del responsable de tratamiento o de las obligaciones propias de las autoridades públicas, los autores Nelson Remolina Angarita, Manuel Tenorio y Gustavo Quintero han señalado la necesidad de que se interprete de forma holística la norma constitucional y se cumpla con una adecuada ponderación de derechos:

> La protección de datos personales en su vertiente de intimidad o de *habeas data* ya sea como obligación, facultad o como derecho debe tener un entorno constitucional total, en el sentido de que se debe visualizar como prerrogativa individual del gobernado o función institucional. Por ejemplo, lo que puede ser la regla del derecho fundamental al *habeas data* prevista en el artículo 15 superior, puede ser una excepción al derecho de petición reglamentado en el artículo 23 constitucional o el acceso a la información del artículo 74 fundamental, todos ellos derechos fundamentales, por lo que la cuestión adquiere magnitudes complejas derivadas de su sincronización constitucional compuesta por varios derechos y facultades a la vez. La interpretación conjunta de esta triple relación entre el titular de los datos personales, el sujeto obligado que los trata y las autoridades que intervienen en esta relación debe ceñirse a un entorno de constitucionalidad de forma total, lo que implica una interpretación holística de la Ley Fundamental.[1206]

[1205] Corte Constitucional de Colombia, "Sentencia C-748/11".

[1206] M.M. TENORIO ADAME, *La protección de datos personales desde el derecho al acceso a la información y como derecho fundamental autónomo, el caso mexicano* (Universidad de los Andes, Facultad de Derecho, núm 1, julio-diciembre de 2012) citado por *N. Remolina Angarita; M. M. Tenorio Adame; G. A. Quintero Navas, De la responsabilidad demostrada en las funciones misionales de la Registraduría nacional del Estado Civil Hacia un programa de gestión de datos personales y la consolidación de un buen gobierno corporativo en el tratamiento de esa clase de información* (Editorial Temis, Colombia, 2018), 30.

En el año 2012 se dicta la Ley 1581 de Protección de Datos Personales que luego de ser sometida a control de constitucionalidad, por parte de la Corte Constitucional de Colombia mediante la sentencia C-748/11, 6 de octubre de 2011, completa el sistema de protección en la República de Colombia, por cuanto establece normas generales aplicables a todo tipo de datos personales.

Esta norma fue reglamentada mediante el Decreto Nacional 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012, publicada en el Diario Oficial 48834, 27 de junio de 2013.[1207]

Pasamos a examinar el contenido esencial del derecho a la protección de datos que como vimos en Colombia se denomina *habeas data*. Sin embargo, debemos señalar que la Corte Constitucional se ha pronunciado señalando que:

> Dentro de las prerrogativas o contenidos mínimos que se desprenden del derecho al *habeas data* encontramos por lo menos las siguientes: (i) el derecho de las personas a conocer –acceso– la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa.[1208]

En la sentencia T-729 de 2002, la Corte explicó la importancia de diferenciar al *habeas data* de otros derechos como el buen nombre y la intimidad, y otorgarle autonomía, principalmente por:

> [...] (i) por la posibilidad de obtener su protección judicial por vía de tutela de manera independiente; (ii) por la delimitación de los contextos materiales que comprenden sus ámbitos jurídicos de protección; y (iii) por las particularidades del régimen jurídico aplicable y las diferentes reglas para resolver la eventual colisión con el derecho a la información.[1209]

Finalmente, normas relacionadas con la protección de este derecho desde otros ámbitos son:

- Ley 1712, 6 de marzo de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.[1210]

[1207] Presidencia de la República de Colombia, "Decreto número 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012", *vLex Global*, 2013, accedido 1 de junio de 2017, https://app-vlex-com.bibliotecavirtual.udla.edu.ec/?r=true#WW/search/content_type:6/Decreto+1377+Reglamenta+parcialmente+la+Ley+1581/WW/vid/445722970.

[1208] Corte Constitucional de Colombia, "Sentencia C-748/11".

[1209] Corte Constitucional de Colombia, "Sentencia T-729/02".

[1210] Congreso de la República de Colombia, *Ley 1712* de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, 2014, accedido 1 de junio de 2017, https://app-vlex-

- Ley 1273, 5 de enero de 2009, mediante la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado, denominado "de la protección de la información y de los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.[1211]

A continuación, se examinarán aquellos elementos que permitirán construir un contenido esencial del derecho a la protección de datos personales en Colombia. El análisis se hará respecto de la normativa vigente, integrando los textos constitucionales y legales de carácter general vigentes a la fecha, y cuando lo justifique el tema abordado, se recurrirá a la normativa sectorial. Además, se utilizará la jurisprudencia constitucional que, en el caso colombiano, es de carácter general y vinculante:

a) Ámbito: Registros o ficheros públicos y privados

De la simple lectura del artículo 15 se desprende que en Colombia el ámbito de protección del *habeas data* es tanto de los ficheros públicos como de los privados, puesto que se mencionan como responsables de los archivos a las entidades públicas y privadas.

En el artículo 2 de la Ley 1266 de 2008, que regula el *habeas data*, consta expresamente que su ámbito de aplicación son las bases públicas y privadas. Ahora bien, dicha ley pese a que pretendía ser de aplicación general a todo tipo de datos, la Corte Constitucional, en sentencia C-1011 de 2008, "dejó claro que la materia de lo que luego se convertiría en la Ley 1266 es solamente el dato financiero y comercial. Por lo tanto, la Ley 1266 solamente puede ser considerada una regulación sectorial del *habeas data*"[1212].

Por su parte, la Ley 1581 de Protección de Datos Personales de 2012, en el artículo 2 también determina el ámbito a entidades de naturaleza pública o privada. La sentencia C-748/11, respecto a lo general o sectorial de la norma, en lo que concierne a datos privados señala que:

> [...] buscaba llenar el vacío de estándares mínimos de protección de todos los datos personales, de ahí que su título sea precisamente «Por el cual se dictan disposiciones generales para la protección de datos personales», concluyéndose que con la introducción de esta reglamentación general y mínima aplicable en mayor o menor medida a todos los datos personales, el legislador ha dado paso a un sistema híbrido de protección en el que confluye una ley de principios generales con otras regulaciones

---

com.bibliotecavirtual.udla.edu.ec/?r=true#WW/search/content_type:6/LEY+1712+COLOMBIA/WW/vid/496520798.

[1211] "Artículo 269F: Violación de datos personales.- El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes". Ver Congreso de la República de Colombia, *Ley 1273*, 5 de enero de 2009, por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado «de la protección de la información y de los datos» y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

[1212] Corte Constitucional de Colombia, "Sentencia C-748/11".

> sectoriales, que deben leerse en concordancia con la ley general, pero que introduce reglas específicas que atienden a la complejidad del tratamiento de cada tipo de dato.

En las dos normas citadas se advierte que se excluye del ámbito de aplicación de la ley a las bases o archivos de seguridad, defensa, inteligencia y contrainteligencia, así como aquellos considerados domésticos. En la Ley 1581 de Protección de Datos Personales se añade las siguientes excepciones: las bases de datos y archivos de información periodística y otros contenidos editoriales; las bases de datos y archivos regulados por la Ley 1266 de 2008 (financieros); las bases de datos y archivos regulados por la Ley 79 de 1993 (censo de población y vivienda); las bases de datos y archivos regulados por la Ley 594 de 2000 (sobre archivos); y las bases de datos y archivos relacionados con el Registro Civil de las Personas.

b) Naturaleza del dato

Respecto de la Ley 1266 de 2008 de *habeas data*, el artículo 3, relativo a las definiciones, reconoce al dato personal como cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Y acerca de este dato se consideran tres subtipos:

i. Dato público. Es aquel que la ley o la Constitución Política los denomina así; pueden ser documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.
ii. Dato semiprivado. El que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar, no solo a su titular, sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
iii. Dato privado. Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular.

En cambio, la Ley 1581 de Protección de Datos Personales de 2012, en el artículo 3, marca únicamente el concepto de dato personal como cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Pero además, esta ley consagra el título III, denominado "Categorías especiales de datos", que incluye otros tipos de datos como los sensibles y los propios de niños, niñas y adolescentes.

La sentencia de la Corte Constitucional declaró exequibles estos artículos aun cuando no mantenía la clasificación de datos que constaba en la Ley 1266 de 2008, por cuanto consideró:

> En primer lugar, la clasificación de los datos personales en públicos, semiprivados y privados o sensibles, es solamente una posible forma de categorizar los datos, pero no la única; otras clasificaciones podrían ser producto de criterios diferentes al grado de aceptabilidad de la divulgación del dato. El legislador, por tanto, tiene libertad para elegir o no elegir una categorización. Ahora bien, es cierto que el propio legislador estatutario adoptó algunas de estas clasificaciones, como la de datos sensibles, cuyo tratamiento se prohíbe con algunas excepciones en el artículo 6 del proyecto. Para poder dar sentido a este precepto, a juicio de la Sala, basta con acudir a las definiciones

> elaboradas por la jurisprudencia constitucional o a las definiciones de otros preceptos legales, como la Ley 1266...[1213].

De lo transcrito se concluye que, si bien no se menciona expresamente el dato inocuo o irrelevante entre los subtipos de datos, la Corte Constitucional determina que se podrá acudir a cualquier categorización bajo la condición de que esta ayude a proteger el derecho.

En el artículo 5 de la ley citada consta descrito el concepto de datos sensibles:

> Artículo 5 Datos sensibles.- Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos".

Mientras que en el artículo 7 de la ley citada, respecto de la categoría denominada datos personales de niños, niñas y adolescentes, se prohíbe expresamente su tratamiento, salvo aquellos datos que sean de naturaleza pública.

Asimismo, la Corte Constitucional colombiana en Sentencia C-748/11 ha precisado que las características de los datos personales son las siguientes:

> i) estar referido a aspectos exclusivos y propios de una persona natural,
> ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos;
> iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y
> iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación.

A lo largo de la norma constitucional y legal existente se utilizan los términos bases de datos y archivos para determinar un conjunto organizado de datos personales que sean objeto de tratamiento, artículo 3 de la Ley 1581 de Protección de Datos.

Respecto del concepto "bancos de datos", la sentencia T-414/92 de la Corte Constitucional colombiana lo ha definido como el "conjunto de informaciones que se refieren a un sector particular del conocimiento, las cuales pueden articularse en varias bases de datos y ser distribuidas a los usuarios de una entidad (administradora) que se ocupa de su constante actualización y ampliación.[1214]

La Corte Constitucional, en la determinación de la exequibilidad de la Ley 1581, analizó sobre el ámbito de protección de dicha norma y al respecto señaló:

> [...] la Sala estima que se ajusta a la Carta, teniendo en cuenta, en primer lugar, que el objeto del derecho al *habeas data* es la protección de los datos personales y, en segundo

[1213] Ibíd.
[1214] Corte Constitucional de Colombia, "Sentencia T- 414 / 92".

> lugar, que efectivamente el proyecto contiene regulaciones generales dirigidas a la protección de todo tipo de dato personal.

De lo transcrito se concluye que aunque la categoría de dato personal inocuo o irrelevante no consta expresamente en la normativa colombiana, esta puede ser parte del ámbito de protección.

Sobre el soporte de los datos no existe una norma específica, únicamente se infiere del artículo 11 de la Ley 1581, Ley de Protección de Datos Personales, que el titular del dato a su criterio podrá solicitar información y esta podrá ser suministrada por cualquier medio, incluyendo los electrónicos. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en su totalidad a aquella que repose en la base de datos. De tal forma que con esta amplia expresión se entiende que se incluye el formato físico y digital.

Finalmente, la protección no solo se refiere a datos automatizados sino que se protege al dato que haya sido tratado con o sin ayuda de la informática, pues la definición que aquí se analiza no se circunscribe únicamente a procedimientos automatizados.[1215]

c) Sujeto activo

Respecto del derecho fundamental contenido en la Constitución colombiana, serán sujetos activos *todas las personas*, al tenor del artículo 15.

Asimismo, la Ley 1266 de 2008 que regula el *habeas data*, señala en el artículo 3 relativo a las definiciones, que el titular de la información será la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos, sujeto del derecho de *habeas data* y demás derechos y garantías contenidas en dicha ley.

La Ley 1581 de Protección de Datos Personales de 2012, por su parte, define al titular como la persona natural, cuyos datos personales sean objeto de tratamiento, conforme el artículo 3.

Por cuanto, uno de los derechos que conforman parte del objeto o bien jurídico propio del *habeas data* es el derecho de información, conforme el artículo 13 de la ley citada, podrá suministrarse información personal a las siguientes personas:

a. A los Titulares, sus causahabientes o sus representantes legales;
b. A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;
c. A los terceros autorizados por el Titular o por la ley. De esta forma definimos también a estos como sujetos activos de este derecho fundamental.

Respecto de la titular del derecho por parte de personas jurídicas, la sentencia de la Corte Constitucional afirma que:

> Por otra parte, llama la atención de la Sala que la definición del literal c) se restrinja a los datos de las personas naturales. Por tanto, la definición pareciera reñir, en principio, con algunos pronunciamientos de esta Corporación en los que se ha admitido que las

[1215] Corte Constitucional de Colombia, "Sentencia C-748/11".

personas jurídicas también pueden ser titulares del derecho al *habeas data*, como la sentencia T-462 de 1997 y C-1011 de 2008. Sin embargo, en sentir de la Sala, no se trata de una restricción que desconozca la doctrina constitucional sobre la protección del *habeas data* en cabeza de las personas jurídicas, ni el principio de igualdad. Ciertamente, la garantía del *habeas data* a las personas jurídicas no es una protección autónoma a dichos entes, sino una protección que surge en virtud de las personas naturales que las conforman. Por tanto, a juicio de la Sala, es legítima la referencia a las personas naturales, lo que no obsta para que, eventualmente, la protección se extienda a las personas jurídicas cuando se afecten los derechos de las personas que la conforman.[1216]

d) Sujeto pasivo

El artículo 15 de la Constitución señala como pasivo o responsables a las entidades públicas y privadas.

La Ley 1266 de 2008, que regula el *habeas data*, señala en el artículo 3 cuatro tipos de responsables:

a) Fuente de información, que es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final.
b) Operador de la información, que es aquella persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios;
c) El usuario, es la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información.
d) La agencia de Información Comercial que es toda empresa legalmente constituida que tenga como actividad principal la recolección, validación y procesamiento de información comercial sobre las empresas y comerciantes específicamente solicitadas por sus clientes.[1217]

Por su parte, el artículo 3 de la Ley 1581 de Protección de Datos Personales de 2012 dispone como sujetos pasivos a:

i. Encargado del Tratamiento, que es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del Tratamiento.
ii. Responsable del Tratamiento, que es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.[1218]

Finalmente, la Corte Constitucional, en su sentencia C-748-11, señala la solidaridad de los responsables o encargados aun cuando la Ley 1581 no lo mencionaba expresamente:

[1216] Ibíd.
[1217] Senado de la República, "Ley hábeas data y manejo de la información contenida en bases de datos personales (Ley 1266 de 2008) - vLex Global".
[1218] Ley protección de datos personales (Ley 1581 de 2012) - vLex Global.

> [...] lo importante para una verdadera garantía del derecho al *habeas data*, es que se pueda establecer de manera clara la responsabilidad de cada sujeto o agente en el evento en que el titular del dato decida ejercer sus derechos. Cuando dicha determinación no exista o resulte difícil llegar a ella, las autoridades correspondientes habrán de presumir la responsabilidad solidaria de todos, aspecto éste sobre el que guarda silencio el proyecto de ley y que la Corte debe afirmar como una forma de hacer efectiva la protección a la que se refiere el artículo 15 de la Carta.

De esta forma se soluciona las diferentes variedades de responsables que constan en las normativas antes transcritas.

e) Objeto o bien jurídico

a. Derecho de información

El artículo 15 de la Constitución hace referencia directa al derecho de información cuando señala que todas las personas tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Asimismo, en la Ley 1266 de 2008 que regula el *habeas data* consta en el artículo 6 los derechos de los titulares de la información, por los cuales se puede acudir ante los operadores de los bancos de datos, a las fuentes de la información y a los usuarios para ejercer ante ellos el derecho fundamental a esta garantía constitucional.

Por su parte, el artículo 8 de la Ley 1581 de Protección de Datos Personales de 2012 determina, entre los derechos de los titulares de los datos, a conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento; asimismo, admite la obligación del responsable del tratamiento o el encargado del tratamiento de informar al titular, con solicitud previa, respecto del uso que le ha dado a sus datos personales.

El artículo 11 de la referida ley precisa cómo deberá ser suministrada la información al titular, esto es cumpliendo características, por ejemplo, ser de fácil lectura, sin barreras técnicas que impidan su acceso y correspondiendo en un todo a aquella que repose en la base de datos. Además, se establece la obligación del Gobierno nacional de establecer la forma en la cual los responsables del tratamiento y encargados del mismo deberán suministrar la información del titular.

Acerca del artículo 12 de la ley en mención, el responsable del tratamiento, al momento de solicitar al titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

a. El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
b. El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
c. Los derechos que le asisten como Titular;
d. La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

Se establece la obligación del responsable del tratamiento de conservar prueba del cumplimiento y, cuando el titular lo solicite, entregarle copia de esta.

El artículo 14 de dicha ley delimita sobre las Consultas que los titulares o sus causahabientes podrán efectuar acerca de la información personal del titular que repose en cualquier base de datos, sea esta del sector público o privado. El responsable o el encargado del tratamiento deberá suministrar, en un máximo de diez (10) días, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular, a través del medio habilitado por el responsable o el encargado del tratamiento.

b. Autodeterminación informativa

Como se vio en líneas anteriores, la autodeterminación informativa como contenido inherente del derecho a la protección de datos, que en Colombia se denomina *habeas data,* es producto de la interpretación de la jurisprudencia constitucional.

En la sentencia C-748/11, la Corte Constitucional determina la existencia de tres líneas interpretativas. La primera, ya superada, sostenía que el *habeas data* fue inicialmente interpretado como una garantía del derecho a la intimidad, por eso se protegían datos limitados a la vida privada y familiar y aquellos considerados sensibles; dicho de otra manera, se defendía la esfera individual de las injerencias arbitrarias que el Estado u otros particulares pudieran realizar. La segunda línea interpretativa, también ya superada, consideraba al *habeas data* como una manifestación del libre desarrollo de la personalidad, con fundamento en su libertad informativa como manifestación de su dignidad. Para 1995, surge una tercera línea interpretativa, que permanece vigente, por la cual el *habeas data* es un derecho autónomo cuyo elemento esencial es la autodeterminación y la libertad informática.[1219]

Para mayor comprensión, se transcribe a continuación como la Corte Constitucional definió el derecho de la siguiente forma: "El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales"[1220]. El contenido descrito a todas luces hace referencia a la autodeterminación informativa.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

Existen tres principios, el de legalidad, el de libertad y el de acceso y circulación restringida que constan en los literales a), c) y f), respectivamente, del artículo 4 de la Ley 1581 de Protección de Datos Personales, por los cuales se puede concluir que este contenido esencial se encuentra presente en la normativa colombiana:

i. Principio de legalidad, por el cual se establece que esta actividad es reglada y debe sujetarse obligatoriamente a lo dispuesto en ella (literal a) del artículo 4 LPD).

[1219] Corte Constitucional de Colombia, "Sentencia C-748/11".
[1220] Ibíd.

ii. Principio de libertad, que determina que los datos personales no podrán ser obtenidos o divulgados sin autorización previa, o en ausencia de mandato legal o judicial que releve el consentimiento (literal c) del artículo 4 LPD).
iii. Principio de acceso y circulación restringida, por el cual el tratamiento se sujeta a los límites derivados de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o la ley, incluida su publicación en internet o medios masivos (literal f) del artículo 4 LPD). En la Ley 1266 de 2008 sobre el *habeas data* se señala en el artículo 4, relacionado con los principios de la administración de datos, el principio de circulación restringida que coincide textualmente con lo constante en su similar de la Ley 1581 de Protección de Datos Personales, pero en el que se añaden a los principios de temporalidad de la información y la finalidad del banco de datos como elementos que limitan el tratamiento de datos.

Respecto de datos sensibles, en la Ley 1581 de Ley Protección de Datos se resuelve que en general no pueden ser tratados a menos que exista disposición legal que lo autorice, conforme señala el artículo 6 de la citada ley. La Corte Constitucional acerca de esta peculiaridad de los datos íntimos indica que:

> [...] la prohibición de su tratamiento, como regla general, no solamente es compatible con la Carta, sino que es una exigencia del derecho a la intimidad y un desarrollo del principio del habeas data de acceso y circulación restringida. No obstante la norma prevé, que en ciertas ocasiones el tratamiento de tales datos es indispensable para la adecuada prestación de servicios —como la atención médica y la educación— o para la realización de derechos ligados precisamente a la esfera íntima de las personas —como la libertad de asociación y el ejercicio de las libertades religiosas y de opinión—, excepciones éstas que responden precisamente a la necesidad del tratamiento de datos sensibles en dichos escenarios, y por tratarse de casos exceptuados que pueden generar altos riesgos en términos de vulneración del habeas data, la intimidad e incluso la dignidad de los titulares de los datos, los agentes que realizan el tratamiento en estos casos, tienen una responsabilidad reforzada que se traduce en una exigencia mayor que también deberá traducirse en materia sancionatoria administrativa y penal.[1221]

Mediante el artículo 10, de la Ley de Protección de Datos, se establecen los casos en los cuales no es necesaria la autorización del titular para la recogida y tratamiento de datos personales y en los que la ley suple dicho consentimiento. Esto es la información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial: datos de naturaleza pública; casos de urgencia médica o sanitaria; tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; datos relacionados con el Registro Civil de las Personas.

d. Principios

Cada sistema normativo puede reconocer principios mínimos para la administración de los datos personales. En este sentido, la normativa y jurisprudencia colombiana reconoce otro principio denominado integridad, por el cual:

[1221] Ibíd.

> [...] se prohibió que el manejo de los datos fuese incompleto, en razón a que esta situación puede distorsionar la veracidad de la información. En dicha oportunidad, la Corte decidió tutelar los derechos de un usuario del sistema financiero que había sido afectado con una información incompleta. Por lo tanto, se ordenó a la entidad administradora de datos, completar la información acerca del comportamiento comercial del actor. En consecuencia, en virtud de aquél principio «*la información que se registre o se divulgue a partir del suministro de datos personales debe ser completa, de tal forma que se encuentra prohibido el registro y divulgación de datos parciales, incompletos o fraccionados. Con todo, salvo casos excepcionales, la integridad no significa que una única base de datos pueda compilar datos que, sin valerse de otras bases de datos, permitan realizar un perfil completo de las personas*» (énfasis en el original) (Sentencia T-729 de 2002).[1222]

i. Deber de información

El literal e) del artículo 4º de la Ley 1581 de 2012, contenida en la Ley de Protección de Datos Personales, establece en los principios para el tratamiento de datos personales, al principio de transparencia que hace alusión al deber de información por el cual debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Este deber de información consta también descrito en el artículo 11 de la referida ley cuando se establece la obligación del titular de las bases de datos de suministrar la información por cualquier medio, incluyendo los electrónicos, a petición del titular. Esta obligación incluye que sea completa, de fácil lectura y sin barreras técnicas que impidan su acceso. Además, instaura la obligación de que el Gobierno nacional establezca la forma en la cual los responsables y encargados del tratamiento suministren la información del titular.

El artículo 12 de la ley citada, y conforme se mencionó cuando se analizó el derecho de información, señala que es deber del responsable de los ficheros informar de manera clara y expresa sobre el tratamiento y finalidad de los datos, así como del carácter facultativo de la respuesta a las preguntas que le sean hechas, sobre todo cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.

ii. Pertinencia

Aunque no existe mención expresa en ninguna de las dos normas analizadas, se puede colegir que su aplicabilidad se manifiesta por medio de otros principios como el de calidad y el de finalidad de los datos.

Así también, de uno de los deberes del responsable del tratamiento que indica que será su obligación actualizar la información, comunicando de forma oportuna al encargado del tratamiento todas las novedades respecto de los datos que previamente le haya suministrado, y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada, conforme el literal f) del artículo 17 y de

[1222] Ibíd.

los literales e) y d) del artículo 18 relativo a las responsabilidades de los encargados del tratamiento.

iii. Calidad

El literal d) del artículo 4.º de la Ley 1581 de 2012, Ley de Protección de Datos Personales, sobre principios para el tratamiento de datos personales establece el principio de veracidad o calidad por el cual la información debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error. Llama la atención en este caso, la prohibición del tratamiento de los fragmentos de datos, toda vez que la minería de datos precisamente atiende al procesamiento de este tipo de datos, y que una vez armados en conjunto pueden propiciar perfiles completos de las personas.

iv. Finalidad

El literal b) del artículo 4º de la Ley 1581 de 2012, Ley de Protección de Datos Personales, menciona entre los principios para el tratamiento de datos personales el relativo a la finalidad, por el que el procesamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular. Esa finalidad debe cumplir con un análisis de ponderación en el que se verifique caso a caso cuando se justifica la recogida de datos. Por eso es que el artículo 10 de la misma ley establece varios casos en que la ley determina justificado realizar la recogida y tratamiento de datos personales sin autorización del titular: cuando es información requerida por una entidad pública; por orden judicial; casos de urgencia médica o sanitaria; por fines históricos, estadísticos o científicos; relacionados con el Registro Civil de las Personas.

v. Seguridad

El literal g) del artículo 4º de la Ley 1581 de Protección de Datos Personales señala, entre los principios para el tratamiento de datos personales, al de seguridad, por el cual se deberán manejar las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de datos personales. Este texto coincide con las obligaciones, tanto de los responsables como de los encargados de tratamientos contenidos en los literales d) e i) del artículo 17, y literales b) y k) del artículo 18 de la referida ley.

vi. Consentimiento

El literal b) del artículo 4º de la Ley 1581 de 2012, Ley de Protección de Datos Personales, menciona entre los principios para el tratamiento de datos personales al relativo a la libertad por el cual el tratamiento solo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin autorización previa, o en ausencia de mandato legal o judicial que releve el consentimiento. Como se lee del texto transcrito, el consentimiento está ligado directamente con el derecho a la autodeterminación informativa, de tal forma que incluso el principio se denomina de libertad.

El artículo 9 de la ley en análisis, sin perjuicio de las excepciones previstas en ella, expone que en el tratamiento se requiere la autorización previa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

Llama la atención que no se trata de cualquier tipo de consentimiento, sino de aquel que cumple con los estándares internacionales, esto es que sea antes de la recogida de información y, además, debidamente informado, de tal forma que la persona titular de los datos conozca completamente de las consecuencias de la recogida, tratamiento y cesión de los datos que entrega.

En el mismo sentido, se ha pronunciado la Corte Constitucional señalando que:

> El consentimiento del titular de la información es un presupuesto para la legitimidad constitucional de los procesos de administración de datos personales, tratándose de un consentimiento calificado: ya que debe ser previo, esto es, que la autorización debe ser suministrada en una etapa anterior a la incorporación del dato; expreso, en la medida que debe ser inequívoco; e informado, toda vez que el titular no sólo debe aceptar el tratamiento del dato, sino también tiene que estar plenamente consciente de los efectos de su autorización. El proyecto desarrolla los casos en que no es necesaria la autorización, específicamente cuando: la información es requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, los datos de naturaleza pública, los casos de urgencia médica o sanitaria, tratamiento autorizado por la Ley para fines históricos, estadísticos o científicos y datos relacionados con el registro civil de las personas, casos éstos en los que existen importantes intereses constitucionales que justifican tal limitación.[1223]

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto:

a. Derecho de acceso

El artículo 1 de la Ley 1581 señala que la presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Si bien el artículo 4 de la Ley 1581 señala los principios para el tratamiento de datos personales, su contenido describe uno de los derechos que corresponde a los titulares para el ejercicio del derecho a la protección de datos personales, esto es el acceso. El literal f) del citado artículo precisa que los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados conforme a la presente ley.

El artículo 18 de la citada ley, relativo a los deberes de los encargados del tratamiento, señala que solo podrá ser accedida por aquellas personas autorizadas.

[1223] Ibíd.

Ahora bien, este derecho se materializa mediante la función de la Superintendencia de Industria y Comercio, por la cual esta podrá ordenar las medidas que sean necesarias para hacer efectivo el derecho de *habeas data*. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos, de conformidad con el artículo 21 de la Ley 1581 en análisis.

b. Derecho de rectificación

El artículo 8 de la Ley 1581 señala entre los derechos de los titulares de los datos: a) Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

El artículo 18 de la Ley 1581 acuerda entre los deberes de los encargados de tratamiento el de realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley, esto es en cumplimiento de los principios de calidad, finalidad, seguridad de los datos, entre otros.

De similar manera, al igual que el caso del derecho de acceso, este podrá ser ejercido mediante una de las funciones de la Superintendencia de Industria y Comercio por la cual podrá ordenar la rectificación, actualización o supresión de los datos personales, de conformidad con el artículo 21 de la Ley 1581 en análisis.

c. Derecho de oposición

El literal e) del artículo 8 de la Ley 1581, Ley de Protección de Datos Personales, fija que los titulares de los datos personales tendrán derecho a revocar la autorización cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el responsable o encargado ha incurrido en conductas contrarias a esta ley y a la Constitución.

Ahora bien, al respecto la Corte Constitucional lo declara inexequible, de tal forma que "el literal e) debe entenderse en el sentido de que el Titular también podrá revocar la autorización y solicitar la supresión del dato, cuando no exista un deber legal o contractual que le imponga el deber de permanecer en la referida base de datos"[1224].

d. Derecho de cancelación

El artículo 8 de la ley en análisis señala los derechos de los titulares de los datos personales, los cuales podrán solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el responsable o encargado ha incurrido en conductas contrarias a esta ley y a la Constitución. Nuevamente, respecto al artículo 8 se debe mencionar lo

analizado por la Corte Constitucional que declara exequible el literal e), puesto que permite al titular del dato solicitar la supresión del dato a su arbitrio, "cuando no exista un deber legal o contractual que le imponga el deber de permanecer en la referida base de datos"[1225].

Por su parte, el literal c) del artículo 18 señala entre los deberes de los encargados de tratamiento el de realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.

Así también, el literal c) del artículo 21, sobre las Funciones de la Superintendencia de Industria y Comercio, determina entre sus funciones la de disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva. De esta manera, existe un mecanismo cautelar en garantía de los posibles daños que podrían causar ciertos datos. Esta cautela en otras legislaciones suele estar asociada directamente al derecho de eliminación, pues de comprobada la naturaleza dañosa del dato o su ilicitud, este debe ser suprimido.

El derecho de supresión podrá ser ejercido por medio de una de las funciones de la Superintendencia de Industria y Comercio, por la cual podrá ordenar la rectificación, actualización o supresión de los datos personales, de conformidad con el artículo 21, literal b) de la Ley 1581 en análisis.

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

No consta norma relativa a la descripción de este derecho; sin embargo, conforme señaló la Corte Constitucional en su sentencia C-748-11:

> Ciertamente, del derecho al habeas data se desprenden no solamente las facultades de conocer, actualizar y rectificar las actuaciones que se hayan recogido sobre el titular, sino también otras como autorizar el tratamiento, incluir nuevos datos, o excluirlos o suprimirlos de una base de datos o archivo. Por tanto, si bien la disposición se ajusta a la Carta, (refiriéndose a la Constitución Colombiana) no debe entenderse como una lista taxativa de las garantías adscritas al derecho.[1226] (El añadido es de la autora).

f. Derecho de consulta al registro general de protección de datos personales

El Registro Nacional de Bases de Datos, que es el directorio público de las bases de datos sujetas a tratamiento que operan en Colombia, en el artículo 25, del capítulo III, declara que el registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos. Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes.

[1225] Ibíd.
[1226] Ibíd., 132.

g. Derecho a indemnización por daños causados

No consta ninguna norma relativa a la descripción de este derecho.

h. Derecho a la confidencialidad

El literal h) del artículo 4 de la Ley 1581 de Protección de Datos Personales declara entre los principios para el tratamiento de datos personales el de confidencialidad, por el cual todas las personas que intervengan en el tratamiento de datos personales, que no tengan la naturaleza de públicos, están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento; pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

De esa forma, se considera al dato personal como de naturaleza confidencial necesitando de autorización del titular o de la ley para su cesión y difusión conforme señala el literal c) del artículo 4 en mención, que se refiere al principio de libertad.

i. Derecho al olvido digital

Al respecto, la sentencia de la Corte Constitucional colombiana establece que no existe derecho al olvido por cuanto:

> La Sala coincide con la decisión adoptada en la T-040 de 2013, en el sentido de considerar que la vulneración del derecho fundamental no es imputable en este caso a Google en tanto no es responsable de producir la información. Adicionalmente, estima necesario señalar que la razón para no acceder a la desindexación consiste en la protección del principio de neutralidad de la red que, como ya se mencionó, solo puede ser restringida en situaciones excepcionales, ya citadas previamente.[1227]

j. Spam

No consta ninguna norma relativa a la descripción de este derecho.

g) Procedimiento

La Ley 1581, Protección de Datos Personales, señala los siguientes procedimientos en garantía de este derecho:

a. *Consultas*: (art. 14) Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado. El Responsable o el Encargado del Tratamiento deberán suministrar la información por medio habilitado para el efecto en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso

[1227] Corte Constitucional de Colombia, "Sentencia T-277/15", 2015, accedido 29 de mayo de 2017, http://www.corteconstitucional.gov.co/relatoria/2015/t-277-15.htm.

podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

b. *Reclamos*: (art. 15) El titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley, podrán presentar un reclamo ante el responsable del tratamiento o el encargado del tratamiento, el cual será tramitado bajo las siguientes reglas:

1. Se formulará mediante solicitud dirigida al responsable del tratamiento o al encargado del tratamiento, con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo. En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.
2. La solicitud se incluirá el reclamo en trámite y el motivo del mismo, en un término no mayor a dos (2) días hábiles en la base de registro. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.
3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

La misma ley, en el artículo 16, señala al agotamiento de vía como requisito de procedibilidad. El titular o causahabiente antes de acudir y presentar reclamo ante la Superintendencia de Industria y Comercio debe elevar queja ante el responsable o el encargado del tratamiento.

h) Acción de tutela (no existe acción constitucional de habeas data *en Colombia)*

Como se vio oportunamente, el *habeas data* en Colombia no es la garantía constitucional, sino el derecho en sí mismo, por lo que en este caso será procedente analizar el artículo 86 de la Constitución. Dado que el *habeas data* o protección de datos personales es un derecho fundamental, la acción constitucional prevista en la Constitución colombiana para la protección de estos es la acción de tutela.

a. Legitimado activo

Conforme señala el artículo 86 de la Constitución colombiana, serán sujetos activos de la acción de tutela de amparo todas las personas, por sí mismas o por quien actúe a su nombre. Por cuanto son titulares del derecho las personas naturales y jurídicas se

comprende que para garantizarlas y solicitar su efectiva tutela lo son también de la acción de amparo.

Conforme el artículo 10 del Decreto 2591 de 1991, la acción de tutela puede ser ejercida por personas naturales ante la vulneración o amenaza de sus derechos fundamentales, personas jurídicas por intermedio de representante legal, del abogado en calidad de apoderado judicial; o el agente oficioso que actúe en nombre de una persona determinada que no esté en condiciones de promover su propia defensa, circunstancia que debe manifestarse en la solicitud y acreditarse procesalmente, defensor del pueblo (como parte del Ministerio público colombiano) o los personeros municipales, en nombre de cualquier persona que se lo solicite, o de la persona que según su juicio se halle en condiciones de desamparo o de indefensión, sin perjuicio del derecho que le asiste a los interesados.[1228]

b. Legitimados pasivos u obligados

El mencionado artículo 86 de la Constitución determina como sujeto pasivo a la autoridad pública cuando sus actuaciones puedan resultar en una vulneración por acción o por omisión de los derechos constitucionales fundamentales, entre ellos el *habeas data*.

Dicho eso, es posible dirigir acción de tutela en contra de particulares aunque excepcionalmente, conforme el artículo 86 de la Constitución colombiana y el artículo 42 del Decreto 2591 de 1991. La Corte Constitucional en sentencia T-251 de 1993 estableció ciertas condiciones indispensables que habilitan presentar esta acción contra particulares, estas son: a) cuando esté encargado de la prestación de cualquier servicio público; b) cuando la acción se dirija contra quien controle efectivamente o fuere el beneficiario real de la situación que motivó la acción, siempre en una relación de subordinación o indefensión; c) cuando aquel contra quien se entabla la acción viole o amenace violar la prohibición a la esclavitud, la servidumbre y la trata de seres humanos; d) cuando la entidad privada sea aquella contra la cual infructuosamente se hubiere hecho la solicitud en ejercicio del *habeas data*; e) cuando se trate de un medio de comunicación al que se pida la rectificación de informaciones inexactas o erróneas no rectificadas o rectificadas de manera indebida; f) cuando el particular actúe en ejercicio de funciones públicas; g) cuando la solicitud sea para tutelar a quien se encuentre en situación de subordinación o indefensión respecto del particular contra el cual se interpuso la acción.[1229]

Del texto anterior, se desprende que precisamente relacionado al derecho de *habeas data* existe una condición expresa que habilita interponer acción de tutela respecto de particulares.

c. Derechos tutelados por el amparo

[1228] L. CARRERA SILVA, "La acción de tutela en Colombia", *Revista IUS*, vol. 5, 27 (2011), accedido 2 de junio de 2017, http://www.scielo.org.mx/scielo.php?script=sci_abstract&pid=S1870-21472011000100005&lng=es&nrm=iso&tlng=es.
[1229] Ibíd.

Como en Colombia no existe acción constitucional de *habeas data*, sino de tutela de amparo, por medio de esta se protegerán todos los derechos fundamentales consagrados en la Constitución colombiana.

d. Procedencia del amparo

Conforme el citado artículo 86 de la Constitución, esta acción de tutela de amparo "solo procederá cuando el afectado no disponga de otro medio de defensa judicial, salvo que aquella se utilice como mecanismo transitorio para evitar un perjuicio irremediable".

e. Procedimiento

El artículo 86 de la Constitución colombiana admite que el procedimiento para presentar acción de tutela de amparo es que el titular de los datos reclame ante los jueces, en todo momento y lugar, mediante un procedimiento preferente y sumario, la protección inmediata de sus derechos fundamentales, cuando crea que estos resulten vulnerados o amenazados por la acción o la omisión de cualquier autoridad pública. "La protección consistirá en una orden para que aquel respecto de quien se solicita la tutela, actúe o se abstenga de hacerlo. El fallo, que será de inmediato cumplimiento, podrá impugnarse ante el juez competente y, en todo caso, éste lo remitirá a la Corte Constitucional para su eventual revisión [...] En ningún caso podrán transcurrir más de diez días entre la solicitud de tutela y su resolución. La ley establecerá los casos en los que la acción de tutela procede contra particulares encargados de la prestación de un servicio público o cuya conducta afecte grave y directamente el interés colectivo, o respecto de quienes el solicitante se halle en estado de subordinación o indefensión".

i) Institucionalidad de protección

La Ley 1581 de Protección de Datos Personales de 2012 otorga a la Superintendencia de Industria y Comercio (SIC)[1230] la competencia de vigilar el tratamiento de datos personales y garantizar que se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

Además, con esta ley se introdujo el Registro nacional de bases de datos, administrado por la SIC para la debida inscripción de las mismas, siempre y cuando contengan datos personales. Asimismo, se faculta a la SIC para imponer sanciones pecuniarias a los responsables del tratamiento de datos que no cumplan las políticas de protección establecidas en la ley, las cuales consisten en multas, suspensión de actividades y suspensión definitiva de las operaciones en caso de que involucren tratamiento de datos.

j) Régimen sancionador

Conforme la Corte Constitucional colombiana:

> Este derecho como fundamental autónomo requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben pender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los

[1230] "Protección de datos personales | Superintendencia de Industria y Comercio", Sitio web institucional de Superintendencia de Industria y Comercio encargada de protección de datos personales en Colombia, accedido 2 de octubre de 2017, http://www.sic.gov.co/proteccion-de-datos-personales.

> sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones.

La jurisprudencia colombiana señala la necesidad de una institucionalidad administrativa aun existiendo un régimen de control judicial, esto debido a que no es suficiente una protección reactiva ante la existencia de un daño inminente o real, sino principalmente una preventiva que evite la transgresión y permita una tutela efectiva del derecho.

Los artículos 22 a 24 que corresponden al capítulo II, titulado de los Procedimientos y Sanciones, señala que una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del responsable o el encargado del tratamiento, se adoptará las medidas o impondrá las sanciones correspondientes.

El artículo 23 señala las sanciones que la Superintendencia de Industria y Comercio podrá imponer a los responsables y encargados del tratamiento, que incluyen multas, suspensión de las actividades relacionadas con el tratamiento, actos correctivos; cierre temporal, inmediato y definitivo de las operaciones relacionadas con el tratamiento incluidos los datos sensibles. Las sanciones indicadas en el presente artículo solo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

Finalmente, el artículo 24 señala los criterios para graduar las sanciones antes descritas, entre los cuales están la dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley; el beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción; la reincidencia en la comisión de la infracción; la resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio; la renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio; y el reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

Esas normas establecen mecanismos o políticas internas efectivas que permiten demostrar la responsabilidad constan en los artículos 26 y 27 del Decreto número 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.

k) Transferencia internacional de datos

El artículo 26 de la Ley 1581 prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de: información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transferencia; versión generada por el usuario biblioteca; intercambio de datos de carácter médico, cuando así lo exija el tratamiento del titular por razones de salud o higiene pública;

transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable; transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad; transferencias necesarias para la ejecución de un contrato entre el titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del titular; transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

> Parágrafo 1º. En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.
>
> Parágrafo 2º. Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008.[1231]

2.4 Paraguay (1992)

La Constitución del Paraguay de 1992 contempla a la intimidad personal y familiar y a la privacidad, la imagen privada y la dignidad como derechos fundamentales reconocidos:

> Artículo 33 - Del Derecho a la Intimidad.- La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas.[1232]

Con espíritu muy similar a lo sucedido en Brasil, se reconoce la protección de datos de las personas, entendida como el derecho-garantía, así denominado *habeas data:*

> Artículo 135 - Del Hábeas Data.- Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.[1233]

Es importante enfatizar la motivación de los constituyentes paraguayos que se destaca por:

[1231] Ley Estatutaria 1581 de 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Accedido: 6 de agosto de 2018. https://www.sisben.gov.co/Documents/Información/Leyes/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf.

[1232] Convención Nacional Constituyente del Paraguay, "Paraguay: Constitución Política de 1992", *Political Database of the Americas*, 1992, accedido 5 de junio de 2017, http://pdba.georgetown.edu/Constitutions/Paraguay/para1992.html.

[1233] Ibíd.

> [...] la especial atención que pusieron en las preocupaciones de sus pares brasileños, y ello se vio reflejado cuando a poco de entrada en vigencia la norma se interpuso un hábeas data contra la policía nacional –por vía penal– para que ésta le exhibiera al peticionante las constancias que sobre su persona obraban en los registros de aquélla, con lo cual se logró ubicar una importante cantidad de documentos sobre la denominada «Operación Cóndor» —de intercambio de prisioneros entre las dictaduras sudamericanas—, donde obraba abundante información sobre desaparecidos y declaraciones de personas respecto de las cuales la policía siempre había negado que hubieran pasado por sus dependencias, formándose, a partir de ellos, los «archivos del horror».[1234]

De lo transcrito, se colige que no existe en Paraguay derecho autónomo e independiente que proteja los datos personales. El *habeas data* no se reconoce como derecho fundamental sino como garantía constitucional del derecho a la intimidad y a la vida privada. En este mismo sentido:

> [...] el hábeas data no es un derecho fundamental stricto sensu, sino que se trata de un proceso constitucional. Es un instrumento procesal destinado a garantizar la defensa de la libertad personal en la era informática. La calidad de los derechos a proteger le otorga la Constitución, que toma al Hábeas Data como un instrumento procesal irremplazable e incondicionado.[1235]

A diferencia de otros países en los que se considera que el *habeas data* mantiene una doble condición: constituir al mismo tiempo derecho y garantía o mecanismo constitucional de tutela, Paraguay señala que únicamente debe ser considerado como proceso constitucional.

Posteriormente, se han dictado varias normas que pretenden proteger los datos personales:

- Ley 1682, 16 de enero de 2001, que reglamenta la información de carácter privado.[1236] Se la considera de carácter sectorial por cuanto solo protege a los datos personales para uso estrictamente privado.
- Ley 1969, 3 de septiembre de 2002, que modifica, amplía y deroga varios artículos de la Ley 1682. Ley 1969, de 3 de septiembre de 2002, que modifica, amplía y deroga varios artículos de la Ley 1682.[1237]

[1234] L. M. BENÍTEZ, "Derecho a la autodeterminación informativa y acción de *hábeas data* en Iberoamérica", en *La acción de hábeas data en el derecho paraguayo* (Chile: Editorial Ius et praxis / Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, 1997), 116.

[1235] M. E. ALMIRÓN PRUJEL, "La acción de hábeas data, garantía constitucional de derechos fundamentales", en *Garantías Constitucionales, apuntes doctrinarios, legislación aplicable y jurisprudencia nacional* (Asunción: Corte Suprema de Justicia del Paraguay, 2004), 122-3.

[1236] Poder Legislativo del Paraguay, "Ley N° 1682 16/01/2001 Reglamenta la Información de carácter privado. Protección de Datos Personales", *Normativa de Acceso - Paraguay - Guía de Archivos y Fondos Documentales IPPDH Mercosur Acervo Documental Cóndor*, accedido 2 de junio de 2017, http://atom.ippdh.mercosur.int/x-normativa-de-acceso-paraguay.

[1237] Poder Legislativo del Paraguay, "Ley N° 1969, de 3 de septiembre de 2002, que modifica, amplía y deroga varios artículos de la Ley N° 1682. Ley N° 1969, de 3 de septiembre de 2002, que modifica, amplía y deroga varios artículos de la Ley N° 1682", *Normativa de Acceso - Paraguay - Guía de Archivos y Fondos Documentales IPPDH Mercosur Acervo Documental Cóndor*, accedido 2 de junio de 2017, http://atom.ippdh.mercosur.int/x-normativa-de-acceso-paraguay.

- Ley Nº 3440, 16 de julio de 2008, que modifica varias disposiciones de la Ley 1160/97, Código Penal y crea un tipo penal que protege la esfera personal íntima de su vida y especialmente su vida familiar o sexual o su estado de salud.[1238]
- Ley 4017, 23 de diciembre de 2010, de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico.[1239]
- Decreto 7369, 23 de septiembre de 2011, por el que se aprueba el Reglamento de la Ley 4017/10 de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico.[1240]
- Ley 4439, 3 de octubre de 2011, que modifica y amplia varios artículos de la Ley 1160/97, Código Penal, artículos 146 b, 146 c, 146 d, 174, 174 b, 175, 175 b y 188, que incluyen nuevos tipos penales relativos al acceso indebido e interceptación de datos personales.[1241]

[1238] "Artículo 143.- Lesión de la intimidad de la persona. 1°.- El que, ante una multitud o mediante publicación en los términos del artículo 14, inciso 3°, expusiera la intimidad de otro, entendiéndose como tal la esfera personal íntima de su vida y especialmente su vida familiar o sexual o su estado de salud, será castigado con pena de multa. 2°.- Cuando por su forma o contenido, la declaración no exceda los límites de una crítica racional, ella quedará exenta de pena. 3°.- Cuando la declaración, sopesando los intereses involucrados y el deber de comprobación que según las circunstancias incumba al autor, sea un medio adecuado para la persecución de legítimos intereses públicos o privados, ella quedará exenta de pena. 4°.- La prueba de la verdad de la declaración será admitida sólo cuando de ella dependiera la aplicación de los incisos 2° y 3°. 5°.- La persecución penal dependerá de la instancia de la víctima." Poder Legislativo del Paraguay, "Ley Nº 3440, de 16 de julio de 2008, que modifica varias disposiciones de la Ley Nº 1160/97, Código Penal.", *SILpy - SISTEMA DE INFORMACIÓN LEGISLATIVA*, accedido 2 de junio de 2017, http://sil2py.senado.gov.py/formulario/FichaTecnicaExpediente.pmf?q=FichaTecnicaExpediente%2F1619.

[1239] Poder Legislativo del Paraguay, "Ley Nº 4017, de 23 de diciembre de 2010, de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico.", *SILpy - SISTEMA DE INFORMACIÓN LEGISLATIVA*, accedido 2 de junio de 2017, http://sil2py.senado.gov.py/formulario/ListarGenerico.pmf.

[1240] Presidencia de la República de Paraguay, "Decreto Nº 7369 "Por el cual se aprueba el reglamento general de la ley nº 4017 'de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico'", *Dirección General de Firma Digital y Comercio Electrónico*, accedido 2 de junio de 2017, https://www.acraiz.gov.py/html/descargas.html.

[1241] "Artículo 146 b.- Acceso indebido a datos. 1° El que sin autorización y violando sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será castigado con pena privativa de libertad de hasta tres años o multa. 2º Como datos en sentido del inciso 1°, se entenderán solo aquellos, que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible.
Artículo 146 c.- Interceptación de datos. El que, sin autorización y utilizando medios técnicos: 1° obtuviere para sí o para un tercero, datos en sentido del Artículo 146 b, inciso 2°, no destinados para él; 2° diera a otro una transferencia no pública de datos; o 3° transfiriera la radiación electromagnética de un equipo de procesamiento de datos, será castigado con pena privativa de libertad de hasta dos años o multa, salvo que el hecho sea sancionado por otra disposición con una pena mayor. Artículo 146 d.- Preparación de acceso indebido e interceptación de datos. 1° El que prepare un hecho punible según el Artículo 146 b o el Artículo 146 c produciendo, difundiendo o haciendo accesible de otra manera a terceros: 1. las claves de acceso u otros códigos de seguridad, que permitan el acceso a datos en sentido del Artículo 146 b, inciso 2°; o 2. los programas de computación destinados a la realización de tal hecho, será castigado con pena privativa de libertad de hasta un año o multa. 2° Se aplicará, en lo pertinente, lo previsto en el Artículo 266, incisos 2° y 3°". Poder Legislativo del Paraguay, "Ley Nº 4439, de 3 de octubre de 2011, que modifica y amplia varias artículos de la Ley Nº 1160/97, Código Penal. Artículos 146 b; 146 c; 146 d; 174; 174 b; 175; 175 b y 188", *SILpy - SISTEMA DE INFORMACIÓN LEGISLATIVA*, accedido 2 de junio de 2017, http://sil2py.senado.gov.py/formulario/FichaTecnicaExpediente.pmf.

- Ley 4868, de Comercio electrónico, 1 de marzo de 2013.[1242]
- Decreto 1165, 27 de enero de 2014, por el que se aprueba el Reglamento de la Ley 4868, de Comercio electrónico, 1 de marzo de 2013.[1243]

Se continuará este estudio examinando aquellos ingredientes que permitirán identificar los elementos que protegen los datos personales. Pero conforme lo señalado, en el caso paraguayo, el contenido esencial estará directamente ligado al derecho a la intimidad, toda vez que:

> El derecho a la intimidad como género que caracteriza la defensa de la privacidad, del honor, la imagen, la reputación, la identidad, entre otros de los derechos ya mencionados, es el fundamento de la garantía que tutela el Hábeas Data. Al ser garantía, es la herramienta procesal que la Constitución dispone para afianzar el cumplimiento de los derechos fundamentales.[1244]

El *habeas data* es garantía del derecho a la intimidad y de derechos conexos directamente asociados a su esfera de protección; no existe derecho fundamental a la protección de datos personales. Los posibles daños que pudieran ocurrir a las personas deben ser valorados desde la perspectiva de la intimidad y sus limitaciones; por eso es que la Corte Suprema de Justicia señala que:

> [...] el hábeas data no autoriza a solicitar la destrucción de un archivo por el solo hecho de contener datos de una persona, siendo de rigor expresar en qué consiste el daño inferido a la imagen o a la intimidad de la persona. El derecho a la intimidad no tiene un carácter absoluto, y debe ser interpretado en concordancia con los otros derechos protegidos por la Constitución, como ser el derecho a la información (art. 28).[1245]

En suma, siendo los ficheros protegidos únicamente aquellos del ámbito oficial o público es evidente que la retirada de información de ellos debe justificarse desde la perspectiva de la información que debe ser registrada en virtud de un interés general y únicamente aquella que por errada, o que afecte derechos fundamentales, tiene la justificación suficiente para ser modificada o eliminada, principalmente a la luz del derecho a la intimidad.

a) Ámbito: Registros o ficheros públicos y privados

De acuerdo con lo declarado en el artículo 135 de la Constitución, se colige que su ámbito de aplicación son registros oficiales o privados de carácter público. En suma, no existe a nivel constitucional protección respecto de ficheros privados.

[1242] Poder Legislativo del Paraguay, "Ley N° 4868, de Comercio electrónico, de 1 de marzo de 2013", *SILpy - SISTEMA DE INFORMACIÓN LEGISLATIVA*, accedido 2 de junio de 2017, http://sil2py.senado.gov.py/formulario/ListarGenerico.pmf.

[1243] Presidencia de la República del Paraguay, "Decreto N° 1165, de 27 de enero de 2014, por el que se aprueba el Reglamento de la Ley N° 4868, de Comercio electrónico, de 1 de marzo de 2013", *Dirección General de Firma Digital y Comercio Electrónico*, accedido 2 de junio de 2017, https://www.acraiz.gov.py/html/descargas.html.

[1244] ALMIRÓN PRUJEL, "La acción de hábeas data", 122.

[1245] Tribunal de Apelación de lo Civil y Comercial de la Capital, Primera Sala del Paraguay, "Acuerdo y sentencia No 84-1998", en *Garantías Constitucionales, apuntes doctrinarios, legislación aplicable y jurisprudencia nacional* (Asunción: Corte Suprema de Justicia del Paraguay, 2004), 690.

Asimismo, el artículo 8° de Ley Nº 1682 de 2001 que reglamenta la información de carácter privado señala que los únicos registros protegidos son los oficiales o privados de carácter público o aquellos en manos de entidades que suministren información sobre solvencia económica y situación patrimonial. Como la defensa de los datos personales en Paraguay se realiza desde el derecho a la intimidad, no existe protección de datos personales en ficheros privados, pese a que el artículo 1 de la citada ley señala que toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado.

b) Naturaleza del dato

Respecto del concepto de dato personal, la norma constitucional contenida en el artículo 135, antes citado, describe que el *habeas data* procede respecto de información o datos sobre sí misma, refiriéndose a la persona natural titular, o sobre sus bienes. Además, serán de aquellos considerados íntimos debido a que el derecho que se tutela mediante la acción de *habeas data* es el derecho a la intimidad.

De igual forma, "a efectos de la procedencia del hábeas data debe entenderse por registro como un repositorio documental ordenado a los efectos de su compulsa, que está librado al servicio público, con la finalidad de brindar certeza o seguridad jurídica como ocurre con los distintos registros que funcionan bajo la dependencia del Poder Judicial"[1246]. No se hace alusión a bases de datos, archivos o términos similares que permitan interpretar que su soporte sea informático.

Dentro de la categorización de datos, la Ley Nº 1682 de 2001 antes citada, señala la existencia de los datos sensibles, que conforme al artículo 4 son:

> Artículo 4°.- Se prohíbe dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables. Se consideran datos sensibles los referentes a pertenencias raciales o étnicas, preferencias políticas, estado individual de salud, convicciones religiosas, filosóficas o morales; intimidad sexual y, en general, los que fomenten prejuicios y discriminaciones, o afecten la dignidad, la privacidad, la intimidad doméstica y la imagen privada de personas o familias.[1247]

A este tipo de datos se los considera confidenciales, de ahí la prohibición para difundirlos o publicitarlos. Apuntala esta postura la jurisprudencia paraguaya, la cual acerca de identificar qué tipos de datos califican como sensibles, señala:

> Cuando los datos personales del accionante del hábeas data no se relacionan en modo alguno con sus ideas políticas, religiosas, gremiales, ideológicas, ni con el comportamiento sexual del actor, ni con su estado de salud, ni con las enfermedades que tiene o ha tenido, ni con datos sociales (color, raza), desde este punto de vista, la información registrada por Inforconf no puede ser calificada como información sensible y no puede, por ende provocar lesión en el derecho a la intimidad del actor.

[1246] Corte Suprema de Justicia del Paraguay, "Auto Interlocutorio No 649-96", en *Garantías Constitucionales, apuntes doctrinarios, legislación aplicable y jurisprudencia nacional* (Asunción: Corte Suprema de Justicia del Paraguay, 2004), 677.

[1247] Poder Legislativo del Paraguay, "Ley Nº 1682 16/01/2001 Reglamenta la Información de carácter privado. Protección de Datos Personales".

Finalmente, el artículo 5 de la Ley 1682-2001 señala un tipo de dato específico de carácter sectorial, denominado datos sobre situación o solvencia patrimonial o económica:

> Artículo 5°.- Los datos de personas físicas o jurídicas individualizadas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales...

c) Sujeto activo

Para la Constitución paraguaya el *habeas data* es una garantía constitucional, por lo que no se determinará en este acápite al titular del derecho sino al legitimado para interponer esta acción. La norma señala expresamente que será toda persona la legitimada para acceder a la información y a los datos sobre sí misma, o sobre sus bienes.

La Corte Suprema de Justicia de Paraguay, en la obra citada, señala que "En América, la fortaleza del proceso constitucional se mide por la finalidad a cumplir como un derecho fundamental que a todos corresponde. Es decir, la libertad de controlar los archivos que contienen datos personales y disponer sobre ellos el destino de la información que utilizan permite extender la figura a personas físicas e ideales, sin acotar la tutela al derecho consagrado en Europa como «autodeterminación informativa», que sólo se interpreta como un derecho humano". De lo que se concluye que en Paraguay los legitimados activos son personas naturales y personas jurídicas.

d) Sujeto pasivo

Tanto los titulares pasivos como los legitimados pasivos del *habeas data* serán los responsables de los registros oficiales o privados de carácter público que contienen datos personales, conforme dispone el artículo 135 de la Constitución.

Así también, serán responsables y por ende legitimados pasivos de *habeas data* las empresas, personas o entidades que almacenan, procesan y difunden registros oficiales o privados de carácter público o que suministren información sobre solvencia económica y situación patrimonial, conforme el artículo 8° de la Ley 1682 de 2001.

e) Objeto o bien jurídico

a. Derecho de información

Respecto del derecho de información, este consta en el artículo 135 de la Constitución del Paraguay en la cual se señala que toda persona tiene derecho a conocer el uso que se le dé a sus datos personales y la finalidad de su recogida.

El artículo 8° de Ley 1682 de 2001 señala que toda persona podrá conocer el uso que se le dé a los datos personales y, además, sobre la finalidad de su registro y uso.

b. Autodeterminación informativa

En el citado artículo 135 de la Constitución se hace referencia al derecho de la persona de solicitar al magistrado competente la actualización, la rectificación o la destrucción de los datos personales, si esos fuesen erróneos o afectaran ilegítimamente sus derechos. De la enunciación de esta norma, no puede colegirse que exista un reconocimiento del derecho a la autodeterminación informativa en la normativa constitucional paraguaya, ya que la acción sigue atada al derecho a la intimidad cuya garantía, aunque no exclusiva pero si primigenia, es el *habeas data*.

Además, no permitirle al titular la decisión libre de entregar y disponer durante todo el proceso de tratamiento sus datos personales implica que esta garantía constitucional del *habeas data* no recoge en su contenido a la autodeterminación informativa. Toda vez que la libertad informativa de eliminar, modificar o actualizar un dato no debe justificarse en la naturaleza errónea del dato personal o en la afectación ilegítima de sus derechos por medio de este, sino principalmente en la simple voluntad de su titular. Por eso, el consentimiento en la entrega de aquellos datos que la ley no ha establecido como de obligatorio registro es el mecanismo fundamental con el cual se materializa la autodeterminación informativa.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

La normativa constitucional del Paraguay señala que los ficheros, materia de regulación, son los considerados *registros oficiales o privados de carácter público*, así como los ficheros privados de carácter público (Ley 1682-2001); es decir, los ficheros y los datos contenidos en ellos están autorizados y regulados por la ley que establece la necesidad de su registro en cumplimiento de un interés general. Por lo que, aun sin decirlo expresamente, están autorizados por la ley el registro de ciertos datos personales y dado que el consentimiento no es la base del sistema, pues no se necesita la autorización del titular sino, por el contrario, el mandato legal de aplicación es la regla general y la excepción el consentimiento.

d. Principios

i. Deber de información

En cuanto al deber que tienen los responsables de los ficheros oficiales o privados de carácter público no existe una expresión específica en la norma constitucional (art. 35 de la Constitución de la República de Paraguay). Ahora bien, como los titulares gozan del derecho de información, en sentido contrario, es propio de un deber de información por parte de los responsables de los ficheros que permita la efectividad de este derecho aunque no conste expresamente reconocido en la normativa.

ii. Pertinencia

En la norma que recoge el *habeas data*, en la Constitución paraguaya, no existe mención expresa al término *pertinencia* identificándolo como principio. Ahora bien, el artículo 7° de la Ley 1682 de 2001, al establecer la obligación de los responsables de los registros de actualizar permanentemente los datos personales sobre situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales para que de acuerdo con la ley puedan difundirse o publicarse, señala que las empresas, personas o entidades que utilizan los servicios de aquellas entidades que los difunden,

tienen la obligación de suministrar la información pertinente a fin de que los datos que aquellas almacenen, procesen y divulguen, se hallen permanentemente actualizados.

Es decir, se establece a la pertinencia como el criterio por el cual se efectiviza la obligación de actualizar los datos.

iii. Calidad

En la norma que recoge el *habeas data* en la Constitución paraguaya no existe mención expresa a este principio.

iv. Finalidad

El artículo 135 de la Constitución de la república del Paraguay establece un aspecto del principio de finalidad, cuando señala que toda persona tiene derecho a conocer sobre la finalidad por la que fue recogida y tratada la información personal del titular.

El artículo 8° de la Ley 1682 de 2001 señala que toda persona podrá conocer la finalidad de la recogida, uso y tratamiento de los datos personales.

Al respecto, la doctrina paraguaya ha señalado que el uso por la que se recaban los datos debe ser tutelado en la medida en la que los datos no pueden ser utilizados con finalidades discriminatorias.

> Con respecto a si los datos son erróneos o afectasen ilegítimamente los derechos de las personas, es necesario aclarar que todo dato tiene por objeto distinguir o sea discriminar: entre quién es solvente y quién es insolvente; quién es buen o mal pagador; quién ha terminado o no sus estudios y en qué nivel; quién tiene antecedentes penales y quién no los tiene. Lo que puede ser discriminatorio no es el archivo, sino el uso que se haga del mismo. La discriminación está prohibida en nuestro sistema constitucional en el artículo 46, y constituye uno de los conceptos fundamentales que subrayan los Tratados Internacionales sobre Derechos Humanos.[1248]

v. Seguridad

En la norma que recoge el *habeas data* en la Constitución paraguaya no existe mención a este principio.

vi. Consentimiento

En la norma que recoge el *habeas data* en la Constitución paraguaya no existe mención a este principio, toda vez que es la ley la que ha establecido los datos que deben ser entregados para conformar los registros oficiales o privados con carácter público, conforme lo señala la Ley 1682 de 2001, Ley 4017, 23 de diciembre de 2010, de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico y el Decreto 7369, 23 de septiembre de 2011, por el que se aprueba el Reglamento de la Ley 4017/10 de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico.

[1248] ALMIRÓN PRUJEL, "La acción de hábeas data", 123-4.

Así por ejemplo, en la normativa sectorial se limita a regular los datos personales contenidos en ficheros oficiales o ficheros privados de carácter público, incluidos los de solvencia económica y situación patrimonial, es decir ficheros autorizados y regulados por la ley, por considerarlos de interés general; en el artículo 5 se señala que podrán ser publicados o difundidos solo cuando sus titulares hubiesen otorgado autorización expresa y por escrito para el efecto.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

a. Derecho de acceso

El artículo 135 de la Constitución paraguaya señala que toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público. De este modo, el derecho de acceso es el primer derecho consagrado en defensa de la intimidad.

Conforme señala la jurisprudencia paraguaya, este acceso se relaciona directamente al derecho a la intimidad en su relación con el derecho a la información tal como se describe en la siguiente transcripción:

> El derecho a la intimidad funciona como excepción al derecho a la información. Como bien se ha dicho, frente al choque de dos derechos fundamentales, debe prevalecer aquel que está más próximo al núcleo de la personalidad y como [...] el derecho a la información es un derecho relaciona1 del hombre con sus semejantes, cederá ante el derecho a la intimidad, al honor y en menor medida a la propia imagen.[1249]

Es menester, citar en esta parte lo señalado por la jurisprudencia paraguaya que respecto del *habeas data* señala una serie de clasificaciones que hacen alusión a cada una de las facultades que les corresponden a los titulares para el ejercicio del objeto, esto es el acceso, la rectificación, la supresión:

> Además también se puede leer en la jurisprudencia una clasificación del Hábeas Data en: l) Hábeas Data Informativo, que a su vez, puede ser: a) Exhibitorio, en virtud del cual se pretende conocer la información misma, o el dato mismo; en otras palabras, qué es lo que ha sido objeto de registración; b) Finalista, por el cual se pretende conocer el uso concreto de tales datos o elementos informativos, en otras palabras: para que se registran dichos datos; 2) Hábeas Data Aditivo, por el cual se pretende agregar datos faltantes en el registro, o simplemente actualizarlos; 3) Hábeas Data Rectificatorio, que, como su denominación lo indica, persigue la corrección de errores en el registro respectivo; 4) Hábeas Data Cancelatorio o Exclutorio, cuyo objetivo es lograr la supresión, eliminación o destrucción del registro de la llamada "información sensible", vale decir, aquella que, sin que esta enumeración pueda ser conceptuada como taxativa o restrictiva, concierne a la intimidad de la persona, como por ejemplo, la información relativa a las ideas políticas, religiosas, gremiales, filosóficas o ideológicas, el comportamiento sexual de los individuos, el estado de salud de las personas, sus enfermedades pasadas y presentes, datos sociales (color, raza, etc.) situación económica, entre otras.[1250]

[1249] Tribunal de Apelación de lo Civil y Comercial de la Capital, Primera Sala del Paraguay, "Acuerdo y sentencia No 84-1998", 695.
[1250] Ibíd.

b. Derecho de rectificación

La última parte del artículo 135 establece que la actualización, la rectificación o la destrucción de los datos constituyen:

> [...] tres peticiones interrelacionadas y vinculadas con la veracidad de la información. Si los datos son falsos se puede optar por su rectificación o su destrucción. Si los datos son verídicos pero incompletos, se puede pedir la actualización de los mismos. Pero no puede solicitarse su rectificación o destrucción si los datos son comprobadamente exactos.[1251]

Ahora bien, no toda información puede ser rectificada sino que debe cumplirse una serie de condiciones, las cuales son explicadas por la Corte Suprema de Justicia:

> Toda persona humana tiene un derecho básico a la intimidad que debe respetarse, y que no puede caer bajo fiscalización de terceros; pero cuando las acciones del individuo van más allá de su órbita personal para entrar a relacionarse con otros, surge una responsabilidad por los actos que el sujeto realiza, que trascienden lo individual, especialmente si ocasiona algún daño, siendo así, resulta lógico que se registren esos datos y que puedan eventualmente tomar carácter público, como un modo de información a los demás miembros de la sociedad, no pudiendo interferirse o restringirse el acopio de esos datos, salvo que se demuestre que los mismos son erróneos o no están actualizados, si no se dan estos extremos, no hay razón para solicitar la rectificación o destrucción de los datos registrados por medio del hábeas data.[1252]

Finalmente, el artículo 7° de la Ley 1682-2001 dice que serán actualizados permanentemente los datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales que, de acuerdo con esta ley, pueden difundirse o publicarse. De esta forma se reconoce el derecho de actualización de forma independiente al de rectificación, ya que la obligación de actualizar y por ende el derecho de los titulares a exigir el cumplimiento de este deber aparece cuando empresas, personas o entidades almacenan, procesan, utilizan servicios y difunden información.

c. Derecho de oposición

No existe derecho de oposición en la normativa paraguaya debido a que esta se basa en la protección al derecho a la intimidad y no en la autodeterminación informativa de los datos personales. En tal sentido, "el Hábeas Data no autoriza a solicitar la destrucción de un archivo por el solo hecho de contener datos de una persona, siendo de rigor expresar en que consiste el daño inferido a la imagen o a la intimidad de la persona. El derecho a la intimidad no tiene un carácter absoluto, y debe ser interpretado en concordancia con los otros derechos protegidos por la Constitución, como ser el derecho a la información (art. 28)".[1253]

d. Derecho de cancelación

[1251] ALMIRÓN PRUJEL, "La acción de hábeas data", 124.
[1252] Corte Suprema de Justicia del Paraguay, "Auto Interlocutorio No 649-96", 691.
[1253] Tribunal de Apelación de lo Civil y Comercial de la Capital, Primera Sala del Paraguay, "Acuerdo y sentencia 84-1998".

El derecho de cancelación consta descrito en el último inciso del artículo 135 de la Constitución del Paraguay que establece la actualización, la rectificación o la destrucción de los datos. Los datos pueden destruirse únicamente cuando estos sean falsos y en contrario sentido, no podrán ser destruidos si los datos son comprobadamente exactos.

Al respecto, la Corte Suprema de Justicia en Auto Interlocutorio No 649/96 indica que:

> Si la persona que ocurre por vía de Hábeas Data, ya conoce el contenido del registro, carece de objeto la primera fase de conocimiento, entrándose directamente en la segunda fase en la que, a los efectos del debido proceso legal deberá observarse el principio de la bilateralidad, esto es, teniendo presente los datos que consten en el registro en cuestión, se comprobará judicialmente su inexactitud para suprimirlos, o rectificarlos o, en la hipótesis de no producirse tal probanza, para su confirmación.[1254]

De la cita realizada, se colige que los datos solo podrán ser cancelados si se prueba su inexactitud, de tal forma que existen procesos sumarios probatorios con esta finalidad.

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

En la norma que recoge el *habeas data* en la Constitución paraguaya no existe mención a este derecho.

f. Derecho de consulta al registro general de protección de datos personales

No existe norma constitucional ni legal que recoja este derecho.

g. Derecho a indemnización por daños causados

No existe norma constitucional ni legal que recoja este derecho.

h. Derecho a la confidencialidad

Los artículos 5, 6, 7, 8 y 9 de la Ley 1682 de 2001 señalan la prohibición de difundir y publicitar datos sensibles, personales y aquellos relativos a la solvencia económica y la situación patrimonial.

Además, la jurisprudencia paraguaya señala que aun respecto de los datos sensibles existe un nivel de decisión sobre qué difundir desde la perspectiva de la intimidad; en este sentido, la jurisprudencia paraguaya señala:

> Dar publicidad a los datos sensibles de la persona (art. 4 de la Ley No. 168 -2001) se refiere a la afectación ilegítima de derechos, lo cual está emparentado con la intimidad de la persona, o su privacidad, a la vez, a su imagen, a los valores familiares, al honor, etc.; en otras palabras aquello que corresponde a cada persona decidir en qué medida va a compartir sus sentimientos, pensamientos y los hechos de su vida personal, todo en

[1254] Paraguay, Corte Suprema de Justicia del Paraguay, "Auto Interlocutorio 649-96".

> consonancia con la Constitución Nacional y los instrumentos internacionales de Derechos Humanos.[1255]

i. Derecho al olvido digital

No existe norma constitucional ni legal que recoja este derecho.

j. Spam

No existe norma constitucional ni legal que recoja este derecho.

g) Procedimiento

La norma constitucional, artículo 135, fija que se podrá solicitar *habeas data*; es decir, la actualización, la rectificación o la destrucción de datos si fuesen erróneos o afectaran ilegítimamente sus derechos ante el magistrado competente. Sobre este procedimiento se describirá más ampliamente en la parte relativa a procedencia y procedimiento del *habeas data*.

h) Habeas data

a. Legitimado activo

Al respecto, se realizó el análisis previamente pues se aclaró que en Paraguay, al no existir el derecho, en este análisis se hizo referencia a la acción de tutela constitucional. Entretanto, la Corte Suprema de Justicia respecto del legitimado activo de la tutela constitucional del habeas data señala:

> En cuanto a la legitimación en una acción de hábeas data, debe evidenciarse, aunque más no fuere de manera sumaria, el contenido del registro o la constancia que afecte los derechos del recurrente, ya que en caso contrario, cualquiera podría solicitar la exhibición de cualquier registro y conocer, ilegítimamente, detalles relativos a terceras personas.[1256]

b. Legitimados pasivos u obligados

Sobre este tema se efectuó el análisis anteriormente aclarando que, al no existir el derecho en Paraguay, se hizo referencia a la acción de tutela constitucional.

c. Derechos tutelados por el habeas data

La norma constitucional que recoge al *habeas data* no señala de forma expresa qué derechos se tutela bajo su órbita, pero conforme señala la jurisprudencia paraguaya, la acción de *habeas data*, como garantía constitucional, protege a la intimidad personal y familiar por intermedio de ella a la imagen, a la honra, la buena reputación, la voz e imagen propias, a la dignidad, al honor y a la identidad personal; además el derecho de rectificación en medios de comunicación social e incluso combate la discriminación.

[1255] Tribunal de Apelación de lo Civil y Comercial de la Segunda Sala, "Acuerdo y sentencia No 160-2001", en *Garantías Constitucionales, apuntes doctrinarios, legislación aplicable y jurisprudencia nacional* (Asunción: Corte Suprema de Justicia del Paraguay, 2004), 724.
[1256] Paraguay, Corte Suprema de Justicia del Paraguay, "Auto Interlocutorio No 649-96".

Siempre desde la perspectiva de ponderación de derechos entre la intimidad y el derecho de información.[1257]

d. Procedencia habeas data

Según lo establecido en el Auto Interlocutorio 649, 25 de junio de 1996, emanado de la Corte Suprema de Justicia, deben reunirse los siguientes requisitos que permiten la admisión de la acción de *habeas data*:

> [...] puede interponerla cualquier persona física o jurídica, afectada por la existencia de datos que pudieran ser erróneos, falsos o indebidamente difundidos (se debe acreditar, aunque sea en forma sumaria el contenido del registro o la constancia que afecte los derechos del recurrente). Su objeto primordial según el artículo 135 de la Constitución, es el conocimiento o la modificación de los datos existentes en el registro en cuestión. El primer requisito que debe acreditarse es que existe algún registro en el que consten datos relativos a una persona. Con respecto a esto debe existir un previo juicio de méritos, ante el magistrado competente, para que se pueda poner en evidencia la legitimidad del reclamo, antes que se pase a una fase de discusión. Establecida la existencia del registro, y los datos relativos a la persona que solicita su examen, se pasa a la segunda etapa, esto es la contrastación de tales datos con los manifestados y justificados por la persona. Finalizada la etapa descripta, la cuestión queda en manos del juez, quien debe realizar una labor meritoria de la validez de las evidencias presentadas a su juzgamiento. Si las anotaciones del registro ilegítimamente afectan los derechos de la persona recurrente, o fuesen erróneos, y en función a ellos, adoptar una decisión que solamente puede tener como contenido: a) No hacer lugar a la petición porque los datos son correctos; b) Disponer, en su caso, la corrección de los datos asentados en el registro, ante la constatación del error existente; y c) Disponer la destrucción de lo que estuviere indebidamente asentado en el registro, supuesto que tales datos, aparte de erróneos, afectaran ilegítimamente los derechos del recurrente.

e. Procedimiento del habeas data

En el artículo 135 de la Constitución del Paraguay no se especifica cuál sería la autoridad competente para entender la acción de *habeas data*, solo menciona la frase "podrá solicitar ante el magistrado competente...".

Ahora bien, de acuerdo con lo señalado en la doctrina paraguaya, liderada por una jueza especializada en la materia, será competente para conocer del *habeas data*:

> La práctica de nuestros tribunales nos señala que esta acción (anterior a la creación de la Mesa de Entrada de Garantías Constitucionales), se interponía indistintamente ante juzgados civiles como penales, dependiendo del contenido de la petición (por ejemplo al solicitar la destrucción de los archivos referentes a la persona peticionante, obrantes en una firma que proporciona informes confidenciales de la iniciación de juicios de contenido patrimonial, se interponía la acción ante un juzgado en lo civil y comercial; sin embargo, al solicitar la actualización o rectificación de datos obrantes en la Policía Nacional o un Centro de Documentación determinado, se interponía la acción ante un juzgado penal). La Mesa de Entrada de Garantías Constitucionales fue creada por la Acordada No 83 de fecha 4 de mayo de 1998, para la ciudad de Asunción, y reglamentada por la resolución No 694 de fecha 3 de marzo de 2000. El 15 de Octubre de 2001, de conformidad a la Acordada No 2271200 1 de fecha 7 de septiembre de

[1257] ALMIRÓN PRUJEL, "La acción de hábeas data", 129.

> 2001, y la Resolución No 9291200 1 de reglamentación, de la Corte Suprema de Justicia, se habilita la Mesa de Entrada de Garantías Constitucionales para las siguientes localidades: a) San Lorenzo, Lambaré y Luque; b) Ciudad del Este y Hernandarias; y c) Encarnación. Dichas reparticiones dependerán directamente de la Corte Suprema de Justicia, bajo la Supervisión de la Jefatura de la Mesa de Entrada de Garantías constitucionales de la Capital.

i) Institucionalidad de protección

No existe institucionalidad de protección en el Paraguay.

j) Régimen sancionador

En la normativa constitucional no existe referencia alguna a un sistema sancionador. Dicho eso, en la norma sectorial, en el artículo 10 de la Ley 1682-2001 constan descritas las sanciones que deberán aplicarse a varios supuestos de transgresión. Este régimen sancionador es de carácter administrativo. Se aplican cuando las personas físicas o jurídicas transgredan las obligaciones que constan descritas en la ley como publicar o distribuir información sobre situación patrimonial, solvencia económica o cumplimiento de obligaciones comerciales, negativa a rectificar o a suministrar información o lo hagan fuera de los plazos establecidos. Las sanciones serán multas económicas que podrán aumentar en caso de reincidencia. Además de la multa, el juzgado ordenará que se efectúen las rectificaciones o supresiones que correspondan, y podrá ordenar también que la sentencia definitiva sea publicada en forma total, parcial o resumida, a costa del responsable. Será competente para la aplicación de las multas el Juzgado en lo Civil y Comercial, en trámite sumario.

k) Transferencia internacional de datos

No existe referencia a este tema en normativa legal ni constitucional.

2.5 Perú (1993)

La Constitución de la República del Perú de 1993 reconoce en el numeral 7, del artículo 2, los derechos al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propia,[1258] pero ante la mención de los servicios informativos y la prohibición de suministrar información da cuenta de otro derecho contenido en el numeral 6 de la señalada norma, este es el derecho a la protección de datos personales:

> Artículo 2.- Toda persona tiene derecho a: [...] 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

De lo transcrito se colige que en Perú se reconoce el derecho a la protección de datos personales limitado a su interrelación con la intimidad personal, de tal manera que si

[1258] "Artículo 2°.- Derechos fundamentales de la persona Toda persona tiene derecho: Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias". Congreso de la República del Perú, "Perú: Constitución Política de 1993 con reformas hasta 2005", *Political Database of the Americas*, 1993, accedido 5 de junio de 2017, http://pdba.georgetown.edu/Constitutions/Peru/per93reforms05.html.

esta pudiere ser afectada no se entregará la información solicitada por su titular. La redacción deja por fuera de la esfera de protección al dato inocuo o irrelevante, y por ende no existe una protección integral de las personas respecto de sus datos. Se concluye que la norma vigente en la Constitución peruana tiene un corte de primera generación ya que ata la protección de los datos personales al derecho a la intimidad y, pese a que consta en numeral aparte y pareciera que contempla un derecho autónomo, la limitación a datos íntimos personales y familiares no permite su independencia como nuevo derecho fundamental.

Asimismo, la Defensoría del Pueblo deberá supervisar los deberes de la administración estatal y la prestación de servicios públicos.[1259] En el artículo 162 de la Constitución de 1993 constan las competencias de la Defensoría del Pueblo, de las cuales es pertinente la relativa a la defensa de derechos, en este caso los derechos contenidos en los numerales 5 y 6 del artículo 2 de la Constitución.

Finalmente, en la Carta Política peruana consta el artículo 200 que determina lo siguiente:

> Artículo 200: Garantías constitucionales: Son garantías constitucionales: [...] 3) La acción de hábeas data, que procede contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el Artículo 2, inciso 5) y 6) de la Constitución.[1260]

Como se aprecia, aunque sea una versión primigenia aún dependiente del derecho a la intimidad, la Constitución del Perú de 1993 "será la primera en tratar de una manera más integral la problemática del acceso y control de la información –pública y personal– pues incorpora al hábeas data como una acción con múltiples objetivos, pero definiendo aparte el contenido del derecho a la protección de los datos"[1261].

Tuvieron que pasar once años para que, mediante la Ley 28237, 31 de mayo de 2004, el Código Procesal Constitucional[1262] derogue a la antigua Ley 26301, 3 de mayo de 1993, y la Ley de Hábeas Data y Acción de Cumplimiento se incluya dentro del ámbito de protección del recurso, todo tipo de datos, formato físico o electrónico, soporte y ficheros públicos o privados.

Dicha norma también reconocía en el *habeas data* no solo el derecho de acceso, sino otras facultades propias del ejercicio de la libertad informativa como son: la rectificación la actualización, la inclusión y la supresión. Así, este proceso constitucional no solo protege la esfera íntima de la persona, sino de toda la información que conforme su voluntad le permita a su arbitrio desarrollar su proceso de autoconstrucción en sociedad.

[1259] Congreso de la República del Perú, "Perú: Constitución Política de 1993 con reformas hasta 2005".
[1260] Ibíd.
[1261] PUCCINELLI, *Tipos y subtipos*, accedido 8 de junio del 2007, http://www.infobaeprofesional.com/adjuntos/documentos/08/0000887.pdf
[1262] Congreso de la República del Perú, "Ley 28237, 31 de mayo de 2004, Código Procesal Constitucional", *Sistema Peruano de Información Jurídica - SPIJ WEB*, accedido 7 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=0&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=28237&xNormaF=28237.

El Tribunal Constitucional por medio de jurisprudencia vinculante en expediente 4739-2007-PHD, 15 de octubre de 2007, determinó que:

> Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos; por tanto, no puede identificarse con el derecho a la intimidad, personal o familiar, ya que mientras éste protege el derecho a la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen.

Es para el año 2011 que se dicta por primera vez una normativa general especializada, Ley 29733, 3 de julio de 2011, de Protección de Datos Personales,[1263] en la cual se desarrolla el marco integral de resguardo de este derecho. Que posteriormente, para el año 2013, por intermedio del Decreto Supremo 003-2013-JUS, 21 de marzo de 2013, se aprueba el Reglamento de la Ley 29733[1264] y se permite precisar y completar este sistema de garantía.

Asimismo, desde el reconocimiento del *habeas data* en la Constitución de 1993 se dictan otras normas que, siendo de carácter general, regulan únicamente la responsabilidad penal por infracciones cuyo bien jurídico tutelado son los datos personales:

- Decreto Legislativo 635, 8 de abril de 1991, Código Penal (arts. 154, 156,157, 161-164, 207).[1265]
- Ley 30096, 22 de octubre de 2013, de Delitos Informáticos.[1266]
- Ley 30171, 10 de marzo de 2014, por la que se modifican los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, de Delitos Informáticos.[1267]

Existe normativa sectorial en abundancia que evidencia las diversas iniciativas que pretenden proteger los datos personales y construir paulatinamente un derecho autónomo, aunque su versión constitucional haya nacido limitada.

[1263] Congreso de la República del Perú, "Ley N° 29733, 3 de julio de 2011, de Protección de Datos Personales", *Archivo Digital de la Legislación del Perú*, accedido 5 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=0&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=29733&xNormaF=29733.

[1264] Presidencia de la República del Perú, "Decreto Supremo N° 003-2013-JUS, 21 de marzo de 2013, por el que se aprueba el Reglamento de la Ley N° 29733", *Ministerio de Justicia y Derechos Humanos del Perú - Normatividad*, accedido 7 de junio de 2017, http://pisaq.minjus.gob.pe:8080/Normatividad/buscarNorma.

[1265] Congreso de la República del Perú; Comisión Revisora delegada para la revisión de los proyectos, "Decreto Legislativo No. 635, 8 de abril de 1991, Código Penal", *Sistema peruano de información jurídica, SPIJ*, accedido 7 de junio de 2017, http://spij.minjus.gob.pe/content/publicaciones_oficiales/img/CODIGOPENAL.pdf.

[1266] Congreso de la República del Perú, "Ley N° 30096, 22 de octubre de 2013, de Delitos informáticos", *Archivo Digital de la Legislación del Perú*, accedido 7 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=0&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=30096&xNormaF=30096.

[1267] Congreso de la República del Perú, "Ley N° 30171, 10 de marzo de 2014, por la que se modifican los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley N° 30096, de Delitos Informáticos", *Archivo Digital de la Legislación del Perú*, accedido 7 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=0&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=30171&xNormaF=30171.

Se enlista a continuación una serie de normas que, si bien no serán materia de análisis por no ser de carácter general y debido a la metodología empleada, no contribuyen de forma precisa a la conformación del contenido esencial del derecho a la protección de datos en Perú; en cambio sí visibilizan una serie de elementos pendientes de desarrollo o profundización:

- Ley 26702, 9 de diciembre de 1996, General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.[1268]
- Ley 27269, 28 de mayo de 2000, de Firmas y Certificados Digitales[1269] (art. 8).
- Ley 27309, 17 de julio de 2000, que incorpora los delitos informáticos al Código Penal.[1270]
- Ley 27489, 28 de junio de 2001. Regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información[1271] (arts. 9 al 18).
- Ley 27806, 3 de agosto de 2002, de Transparencia y Acceso a la Información Pública.[1272]
- Decreto Supremo 072-2003-PCM, 7 de agosto de 2003, por el que se aprueba el Reglamento de la Ley 27806.[1273]
- Ley 28493, 18 de marzo de 2005, que regula el uso del correo electrónico comercial no solicitado (SPAM),[1274] artículos 1 y 3.
- Decreto Supremo 031-2005-MTC, 4 de enero de 2006, por el que se aprueba el Reglamento de la Ley 28493.[1275]

[1268] Congreso de la República del Perú, "Ley Nº 26702, 9 de diciembre de 1996, General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros", *Archivo Digital de la Legislación del Perú*, accedido 7 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=0&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=26702&xNormaF=26702.

[1269] Congreso de la República del Perú, "Ley Nº 27269, 28 de mayo de 2000, de Firmas y Certificados Digitales", *Archivo Digital de la Legislación del Perú*, accedido 7 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=0&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=27269&xNormaF=27269.

[1270] Congreso de la República del Perú, "Ley Nº 27309, 17 de julio de 2000, que incorpora los delitos informáticos al Código Penal", *Archivo Digital de la Legislación del Perú*, accedido 7 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=0&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=27309&xNormaF=27309.

[1271] Congreso de la República del Perú, "Ley Nº 27489, 28 de junio de 2001. Regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información", *Archivo Digital de la Legislación del Perú*, accedido 7 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=0&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=27489&xNormaF=27489.

[1272] Congreso de la República del Perú, "Ley Nº 27806, 3 de agosto de 2002, de Transparencia y Acceso a la Información Pública", *Archivo Digital de la Legislación del Perú*, accedido 7 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=0&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=27806&xNormaF=27806.

[1273] Presidencia de la República del Perú, "Decreto Supremo Nº 072-2003-PCM, 7 de agosto de 2003, por el que se aprueba el Reglamento de la Ley Nº 27806", *Sistema Peruano de Información Jurídica - SPIJ WEB*, accedido 7 de junio de 2017, http://spij.minjus.gob.pe/libre/main.asp.

[1274] Congreso de la República del Perú, "Ley Nº 28493, 18 de marzo de 2005, que regula el uso del correo electrónico comercial no solicitado (SPAM)", *Archivo Digital de la Legislación del Perú*, accedido 7 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=0&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=28493&xNormaF=28493.

- Ley 29499, 19 de enero de 2010, que establece la vigilancia electrónica personal.[1276]
- Ley 30024, 22 de mayo de 2013, por la cual se crea el Registro Nacional de Historias Clínicas Electrónicas.[1277]
- Decreto legislativo 1353, 7 de enero de 2017, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de gestión de intereses, que modifica la Ley 29733.[1278] El Decreto Supremo Nº 019-2017-JUS de 2017[1279] reglamenta el Decreto Legislativo y en su artículo 2º crea la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, que depende jerárquicamente del Despacho Viceministerial de Justicia.[1280]

Sobre otras normas sectoriales actualizadas de menor jerarquía, se puede revisar el Sistema Peruano de Información Jurídica en la sección de búsqueda por materias, en el apartado Derecho informático, tema Protección de Datos e Información.[1281]

a) Ámbito: Registros o ficheros públicos y privados

Conforme señala el numeral 6 del artículo 2 de la Constitución del Perú de 1993, relativo al derecho a la protección de datos personales, en concordancia con el artículo 200, acerca del proceso constitucional de *habeas data*, se determina que el ámbito de aplicación del derecho a la protección de datos personales era los ficheros públicos y privados.[1282]

El problema radica en la determinación de los responsables que deben cumplir con las obligaciones impuestas en garantía del derecho a la protección de datos personales. La

[1275] Presidencia de la República del Perú, "Decreto Supremo Nº 031-2005-MTC, 4 de enero de 2006, por el que se aprueba el Reglamento de la Ley Nº 28493", *Sistema Peruano de Información Jurídica - SPIJ WEB.*, accedido 7 junio 2017, en http://spij.minjus.gob.pe/libre/main.asp.

[1276] Congreso de la República del Perú, "Ley Nº 29499, 19 de enero de 2010, que establece la vigilancia electrónica personal.", *Archivo Digital de la Legislación del Perú*, accedido 7 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=3&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=635&xNormaF=635.

[1277] Congreso de la República del Perú, "Ley Nº 30024, 22 de mayo de 2013, por la que se crea el Registro Nacional de Historias Clínicas Electrónicas", *Archivo Digital de la Legislación del Perú*, accedido 7 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=0&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=30024&xNormaF=30024.

[1278] Congreso de la República del Perú, "Decreto Legislativo No. 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de gestión de intereses", *Archivo Digital de la Legislación del Perú*, accedido 5 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=3&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=1353&xNormaF=1353.

[1279] Presidencia de la República del Perú, Reglamento del Decreto Legislativo N° 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses, accedido el 27 de agosto de 2019, https://www.gob.pe/institucion/midis/normas-legales/9641-019-2017-jus

[1280] Sitio web de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, https://www.minjus.gob.pe/dgtaipd/

[1281] *Código Procesal Constitucional*, accedido 7 de junio de 2017, http://spij.minjus.gob.pe/libre/main.asp.

[1282] Congreso de la República del Perú, "Perú: Constitución Política de 1993 con reformas hasta 2005".

citada norma menciona que son los servicios informáticos, computarizados o no, públicos o privados, los obligados a no suministrar informaciones que afecten la intimidad personal y familiar.

Posteriormente, el artículo 61 de la Ley 28237, 31 de mayo de 2004, Código Procesal Constitucional, al referirse al *habeas data*, menciona expresamente que se protegerán aquellos datos que se generen, produzcan, procesen o posean en ficheros públicos y privados. La citada norma determina que el *habeas data* procederá en defensa de los derechos constitucionales relativos a la protección de datos personales y de la intimidad respecto de datos en poder de cualquier entidad pública y también de aquellos almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros.

La Ley 29733-2011, de Protección de Datos Personales, señala en el artículo 3 que el ámbito de aplicación de la ley son los ficheros regentados por la administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. El artículo 2 de las definiciones señala que existen bancos de datos personales de administración privada, que son aquellos cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.[1283]

Además, especifica los casos de excepción en los cuales no es aplicable la presente ley, estos son los bancos de datos personales: a) creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar; b) generados para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito.

b) Naturaleza del dato

El numeral 6 del artículo 2 de la Constitución de la República del Perú protege la información de una persona que afecte su intimidad personal o familiar. Esta forma de redacción desconoce expresamente otro tipo de datos que deben ser protegidos, especialmente al dato inocuo con el cual se puede, luego de un tratamiento de datos, construir perfiles de personalidad que pueden causar graves daños no solo a la intimidad personal y familiar, sino a otros derechos fundamentales por la posibilidad de generar discriminación.

Once años después, el artículo 61 de la Ley 28237 de 2004, Código Procesal Constitucional que desarrolla el proceso de *habeas data*, se determina un contenido que amplía la consideración limitada a la intimidad cuando señala que se protegerá la información, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que la administración pública tenga en su poder, cualquiera que sea la forma de expresión: gráfica, sonora, visual, electromagnética o que obre en cualquier otro tipo de soporte material. Anotándose que la información o datos referidos a la persona se encuentran almacenados o registrados en forma manual, mecánica o informática, en

[1283] Congreso de la República del Perú, "Ley N° 29733".

archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros.

Posteriormente, en la Ley de Protección de Datos Personales de 2011 se complementa el sistema de protección mediante las siguientes definiciones relativas a bancos de datos personales, bancos de datos personales de administración privada, bancos de datos personales de administración pública, datos personales, datos sensibles y fuentes accesibles.[1284]

Es decir, se protege el dato personal, entendido como toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados (numeral 4 del artículo 2 de la Ley de Protección de Datos Personales), en cualquier forma de expresión y tipo de soporte que se presenten, ya sean estos materiales, mecánicos o virtuales. Incluido el dato suelto no automatizado, con lo cual esta legislación, en este tema específico, se encuentra a la vanguardia de protección, conforme consta en el numeral 1 del artículo 2 citado. Finalmente, existe una mención expresa al concepto de datos sensibles contemplado en el numeral 5 del artículo 2 de la ley mencionada.

c) Sujeto activo

En el artículo 2 de la Constitución, al referirse al derecho de forma general, se establece como su titular a *toda persona*. Asimismo, el artículo 61 de la Ley 28237 de 2004, Código Procesal Constitucional, vuelve a utilizar la frase *toda persona*.

Finalmente, el artículo de la Ley de Protección de Datos de 2011 señala en el numeral 14 del artículo 2 relativo a las definiciones que será titular de los datos, la persona natural a quien corresponde dicha información.

De esta forma, aunque la expresión que consta en la norma constitucional contraria a la legal, hace alusión a una frase genérica que permite, de primera vista, concluir que son titulares tanto personas naturales como jurídicas; sin embargo, la jurisprudencia zanja

[1284] El artículo 2. Definiciones.- Para todos los efectos de la presente Ley, se entiende por:
1. Banco de datos personales. Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.
2. Banco de datos personales de administración privada. Banco de datos personales cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.
3. Banco de datos personales de administración pública. Banco de datos personales cuya titularidad corresponde a una entidad pública.
4. Datos personales. Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.
5. Datos sensibles. Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual [...]
9. Fuentes accesibles para el público. Bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso. Las fuentes accesibles para el público son determinadas en el reglamento.
Ibíd.

esta duda y determina que este derecho les corresponde tanto a la persona natural como a la persona jurídica.

La sentencia en mención corresponde a la dictada en el expediente 4739-2007-PHD, cuya parte pertinente señala:

> Asimismo, este tribunal se ha pronunciado respecto de cuáles son los derechos fundamentales cuya titularidad pueden ostentar las personas jurídicas. Así bajo una interpretación extensiva del inciso 17) del artículo 2° de la Constitución, toda persona jurídica puede tener un retener para sí aquellos derechos de carácter fundamental que le resulten aplicables. En este sentido, mediante la sentencia de fecha del 4 de agosto de 2006 recaída en el expediente 4972-2006PA/TC este tribunal ha señalado de manera enunciativa una serie de derechos fundamentales invocados para las personas jurídicas entre los que encontramos el derecho a la autodeterminación informativa (apartado e) del Fundamento No. 14).[1285]

En conclusión, son titulares activos del derecho a la protección de datos personales tanto la persona natural como la jurídica, pero como no se menciona ni en la norma constitucional ni legal a la persona jurídica pública, esta se excluye.

d) Sujeto pasivo

La norma constitucional, en el numeral 6 del artículo 2, estableció durante mucho tiempo que el sujeto pasivo de este derecho era el que proveía de servicios informáticos, computarizados o no, públicos o privados, obligados a no suministrar informaciones que afecten la intimidad personal y familiar; es decir, el problema radicaba en la determinación de qué debía entenderse como servicios informáticos. En ese sentido,

> [...] resulta muy imprecisa, tanto sobre el tipo de institución u organización incursa en esta disposición constitucional como sobre la actividad involucrada. Y es que la expresión «servicios informáticos», con relación al tratamiento de los datos personales, podría dar a entender que la protección de este derecho se extiende exclusivamente a las entidades públicas o privadas que proporcionan este tipo de información a terceros («servicios»), pudiendo quedar excluidos los registros o bancos de datos existentes que no brindan servicio ni acceso al público.[1286]

Posteriormente, el artículo 61 de la Ley 28237, 31 de mayo de 2004, Código Procesal Constitucional, al referirse al *habeas data*, señala expresamente que se protegerán aquellos datos que se generen, produzcan, procesen o posean en ficheros públicos y privados. La citada norma determina que el *habeas data* procederá en defensa de los derechos constitucionales relativos a protección de datos personales y de intimidad respecto de datos en poder de cualquier entidad pública y también de aquellos almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros.

[1285] Sala Primera del Tribunal Constitucional del Perú, "Expediente No. 4739-20007-PHD".
[1286] F. J. E. PRAELI, "El derecho a la protección de los datos personales: Algunos temas relevantes de su regulación en el Perú", *THĒMIS-Revista de Derecho*, vol. 0, 67 (2015), accedido 9 de junio de 2017, http://revistas.pucp.edu.pe/index.php/themis/article/view/14462.

En el artículo 2 de la Ley de Protección de Datos Personales de 2011 se señala, entre las definiciones, como sujetos pasivos al titular y al encargado del banco de datos personales.

Las personas naturales, personas jurídicas de derecho privado o entidades públicas son titulares de los bancos de datos personales cuando determinan la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad; mientras que los encargados son aquellos que solos, o actuando conjuntamente con otros, realizan el tratamiento de los datos personales por encargo del titular del banco de datos personales.[1287]

Finalmente, en el artículo 30 de la citada ley consta que por cuenta de terceros se pueden prestar servicios de tratamiento de datos personales. Quienes no pueden aplicar o utilizar con un fin distinto al que figura en el contrato o convenio celebrado ni ser transferidos a otras personas, ni aun para su conservación. Una vez ejecutada la prestación materia del contrato o del convenio deberán suprimir los datos salvo autorización expresa.

e) Objeto o bien jurídico

a. Derecho de información

El artículo 18 de la Ley de Protección de Datos Personales consagra expresamente el derecho de información del titular, que consiste en:

> [...] ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del encargado del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello. Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables.

Este derecho se materializa en el momento de la recogida de la información cuando se solicita el consentimiento: para el tratamiento (art. 13); para el flujo transfronterizo de datos (art. 15) y para relevar al responsable de la obligación de confidencialidad (art. 18).

b. Autodeterminación informativa

Conforme el numeral 6 del artículo 2 de la Constitución de la República del Perú de 1993 se protege la información de una persona que afecte su intimidad personal o familiar. Como se vio en líneas precedentes, esta redacción establecía una limitación al derecho, pues no protege el dato personal por sí mismo, sino que lo asocia de manera

[1287] Congreso de la República del Perú, "Ley N° 29733".

innecesaria a la necesidad de determinar la transgresión de la intimidad, negando desde esta perspectiva el derecho a la autodeterminación informativa, contenido esencial del derecho a la protección de datos personales.

Ante esta evidente limitación, el Tribunal Constitucional del Perú en expediente No. 1797-2002-HD/TC de 29 de enero de 2003, reconoce a la autodeterminación informativa con un contenido distinto del derecho a la intimidad, la imagen e incluso de la identidad, conforme consta en la transcripción a continuación:

> Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2° de la Constitución. Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen. Tampoco el derecho a la autodeterminación informativa debe confundirse con el derecho a la imagen, reconocido en el inciso 7) del artículo 2° de la Constitución, que protege, básicamente la imagen del ser humano, derivada de la dignidad de la que se encuentra investido; mientras que el derecho a la autodeterminación informativa, en este extremo, garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado, a efectos de preservar su imagen derivada de su inserción en la vida en sociedad. Finalmente, también se diferencia del derecho a la identidad personal, esto es, del derecho a que la proyección social de la propia personalidad no sufra interferencias o distorsiones a causa de la atribución de ideas, opiniones, o comportamientos diferentes de aquellos que el individuo manifiesta en su vida en sociedad. En ese sentido, por su propia naturaleza, el derecho a la autodeterminación informativa, siendo un derecho subjetivo tiene la característica de ser, prima facie y de modo general, un derecho de naturaleza relacional, pues las exigencias que demandan su respeto, se encuentran muchas veces vinculadas a la protección de otros derechos constitucionales...[1288].

En el mimo sentido, el Tribunal Constitucional Perú dictó sentencia en el Expediente 4739-2007-PHD, 15 de octubre de 2007, en el cual se hace hincapié en los distintos ámbitos de protección que tienen la intimidad, la privacidad y la autodeterminación informativa, de acuerdo con el texto que a continuación se transcribe:

> El derecho a la autodeterminación informativa consiste en una serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentran estrechamente ligados a un control sobre la información como una autodeterminación de la vida íntima de la esfera personal. Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente a los derechos que le conciernen a su esfera personalísima, sino a la persona en la totalidad de los ámbitos, por tanto no puede identificarse con el derecho la intimidad personal o familiar, ya que mientras este protege el derecho la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso, revelación de los datos que le concierne. En este sentido se ha pronunciado este Colegiado en la sentencia recaída en el expediente No. 1797-2002 HD/TC de 29 de enero de 2003. En este orden de ideas el derecho a la autodeterminación informativa protege el titular de

[1288] Tribunal Constitucional del Perú, "Expediente 1797-2002-HD".

> los mismos frente a los posibles abusos o riesgos derivados de la utilización de los datos, brindando el titular afectado la posibilidad de lograr la exclusión de los datos que considere "sensibles" y que no deben ser objeto de difusión y de registro; así como le otorga la facultad para poder oponerse a la transmisión y difusión de los mismos...[1289].

Esta posición jurisprudencial fue reconocida en el artículo 61 de la Ley 28237 de 2004, Código Procesal Constitucional, que soluciona esta perspectiva inicial acotada, por la cual solo se protegía la no difusión de la información personal íntima. Ya que la citada normativa ahora faculta al titular a acceder, conocer, actualizar, suprimir, incluir o rectificar sus datos personales sin la necesidad de que esta información afecten o hayan afectado la intimidad personal o familiar, de esta forma se garantiza en Perú un contenido adecuado del derecho a la protección de datos personales que ya incluye al derecho a la autodeterminación informativa.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

La Ley de Protección de Datos Personales, en el artículo 13, relativo al alcance del tratamiento de datos personales, señala la necesidad de norma legal para el tratamiento que no sea autorizado por su titular (núm. 5); asimismo la ley deberá dictarse respetando su contenido esencial y justificarse en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos (núm. 2).

Ahora bien, respecto de las limitaciones y alcances al ejercicio del derecho fundamental a la protección de datos personales consta en el artículo 13 antes citado lo siguiente: a) se necesita de reglamento que determine medidas especiales para el tratamiento de los datos personales de los niños y de los adolescentes (núm. 3); b) se requiere de mandamiento motivado del juez o autorización de su titular para abrir, incautar, interceptar o intervenir comunicaciones, telecomunicaciones, sistemas informáticos o sus instrumentos (núm. 4); c) se necesita de ley para el tratamiento de datos sensibles, siempre que ello atienda a motivos importantes de interés público (núm. 6); se requiere norma expresa o convenio de encargo conforme la Ley Administrativa, para el tratamiento por parte de entidades públicas competentes relativos a la comisión de infracciones penales o administrativas (núm. 8).

No se requiere consentimiento del titular y está autorizado por el artículo 14 de la citada Ley 29733 los siguientes casos: 1. cuando se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias; 2. Cuando estén contenidos o destinados a ser contenidos en fuentes accesibles para el público; 3. Relativos a solvencia patrimonial y de créditos; 4. Medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos regulados por la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privadas en los servicios Públicos, o la que haga sus veces; cuando sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte; cuando se deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento; 6. Relativos a salud y sea necesario en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular; cuando medien razones de salud pública; para la realización de estudios epidemiológicos o análogos, en tanto se aplique disociación; 7. Efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o

[1289] Sala Primera del Tribunal Constitucional del Perú, "Expediente 4739-20007-PHD".

sindical sobre sus miembros; 8. Aplicado anonimización o disociación; 9. Salvaguardar intereses legítimos del titular de datos personales.

d. Principios

i. Deber de información

Así pues, el artículo 2 numeral 6 de la Constitución del Perú, respecto del deber de información, señala la prohibición expresa de los servicios informáticos, computarizados o no, públicos o privados de suministrar informaciones que afecten la intimidad personal y familiar. Es decir, durante varios años no existió en Perú el deber de información ni como derecho ni como principio.

Es mediante la Ley de Protección de Datos Personales de 2011 que el artículo 18, al describir el derecho de información del titular de datos personales, determina los deberes de los titulares de los ficheros públicos y privados respecto de cada una de las obligaciones que deben cumplir en garantía del derecho a la protección de datos personales. Como por ejemplo, el deber de informar al titular del dato sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del encargado del tratamiento de sus datos personales, entre otros más específicos descritos en la cita pertinente.

ii. Pertinencia

La referencia a la pertinencia se toma como parte del principio de calidad de datos, contenido en el artículo 8 de la Ley de Protección de Datos Personales. Esta condición específica de los datos consta descrita en el artículo 20 de la ley citada, pues faculta al titular de los datos a ejercer su derecho de actualización, inclusión, rectificación y supresión cuando, entre otras causas, hayan dejado de ser necesarios o pertinentes a la finalidad para la cual fueron originalmente recopilados o cuando hubiera vencido el plazo establecido para su tratamiento.

Por eso es que el numeral 3 del artículo 28 de la ley en análisis, relativo a las obligaciones propias del responsable de un fichero señala que solo podrán recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido.

Asimismo, consta en el numeral 7 del mismo artículo 28 entre las obligaciones del responsable del fichero la de suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiesen vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación. Esta norma se desarrolla desde la perspectiva de la obligación del responsable del fichero lo que consta, en cambio, desde el matiz de los derechos de los titulares para ejercitar sus acciones de actualización, inclusión, rectificación y supresión.

iii. Calidad

El artículo 8 de la Ley de 2011 en mención reconoce el principio de calidad por el cual los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento. Este principio de calidad significa en general un deber de diligencia que mantenga en todo momento un dato que cumpla con todas las características antes citadas.

iv. Finalidad

El artículo 6 de la Ley de Protección de Datos Personales señala que el principio de finalidad establece que los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

Este principio coincide y se manifiesta expresamente en los numerales 3, 4 y 7 del artículo 28 desde la perspectiva de las obligaciones de un responsable de fichero, por las cuales solo pueden recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido, así como la prohibición de utilizar datos personales para finalidades distintas de aquellas que motivaron su recopilación o el deber de suprimirlos cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiesen vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación.

Finalmente, este principio tiene estrecha vinculación con el de calidad de datos como se revisó previamente, debido a que si se incumple la finalidad para la cual se recogieron los datos se afecta directamente a la calidad de ellos.

v. Seguridad

El artículo 9 de la Ley de Protección de Datos Personales señala el principio de seguridad como aquel por el cual el titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

Por su parte, el artículo 16 de la citada ley señala que para fines del tratamiento de datos personales, el responsable del banco de datos personales debe adoptar las mencionadas medidas técnicas, organizativas y legales con la finalidad de evitar su alteración, pérdida, tratamiento o acceso no autorizado. Por cuanto en Perú existe la entidad responsable del control del tratamiento de datos personales, los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes.

vi. Consentimiento

El artículo 5 de la Ley de Protección de Datos Personales señala que para el tratamiento de los datos personales debe mediar el consentimiento de su titular. En cambio, el artículo 13 numeral 5 de la citada ley determina que los datos personales solo pueden ser objeto de tratamiento con el consentimiento de su titular, salvo ley que lo faculte de forma expresa. Además, se determina como características del consentimiento que este debe ser previo, informado, expreso e inequívoco.

En ese sentido, el numeral 6 del artículo 13 de la norma en mención, determina que en el caso de datos sensibles, el consentimiento para efectos de su tratamiento, además de los requisitos previamente enunciados, deberá efectuarse por escrito. Aun cuando no mediara el consentimiento del titular, el Sistema Peruano de Información Jurídica tratamiento de datos sensibles puede efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes de interés público.

El numeral 7 del artículo 13 admite que el titular de datos personales puede revocar su consentimiento en cualquier momento, observando al respecto los mismos requisitos que con ocasión preste su otorgamiento. Este contenido, aunque se refiere a revocatoria de consentimiento, en realidad permite la aplicación del derecho de oposición.

Finalmente, el artículo 28 de la Ley de Protección de Datos Personales señala que entre el responsable del fichero y el encargado del tratamiento del banco de datos personales serán responsables de efectuar el tratamiento de datos personales, solo con el consentimiento informado previo, expreso e inequívoco del titular de los datos personales, salvo ley que lo autorice o los casos señalados en el artículo 14 de la presente ley que se analizará a continuación.

vii. Limitaciones al consentimiento

Las limitaciones al consentimiento constan descritas en el artículo 14 de la Ley de Protección de Datos Personales, por el cual no se requiere el consentimiento del titular de datos personales para el tratamiento de datos personales cuando:

a) los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias;
b) se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público;
c) se refiera a datos personales relativos a la solvencia patrimonial y de crédito, conforme a la ley;
d) medie norma para la promoción de la competencia siempre que la información no sea utilizada en perjuicio de la privacidad del usuario;
e) los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte;
f) se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento;
g) se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular;

h) el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos;
i) se hubiera aplicado un procedimiento de anonimización o disociación;
j) el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos por parte del titular o el encargado de datos personales;
k) otros establecidos por ley o por el respectivo reglamento.

viii. Otros principios

La Ley de Protección de Datos Personales del Perú señala entre sus principios los siguientes:

- El artículo 4, relativo al principio de legalidad, por el cual el tratamiento de los datos personales se hace conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.
- El artículo 7, respecto del principio de proporcionalidad, que determina que todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.
- El artículo 10, sobre el principio de disposición de recurso, que señala que todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.
- El artículo 11, sobre el principio de nivel de protección adecuado, aplicable al flujo transfronterizo de datos personales, garantiza un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta ley o por los estándares internacionales en la materia.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

La normativa peruana de protección de datos personales reconoce los derechos de información, acceso, rectificación, oposición, entre otros. Además, los artículos 26 y 27 de la citada ley declaran que ante los bancos de datos personales, regentados por la administración pública, es posible negar las referidas acciones por razones justificadas en la protección de derechos e intereses de terceros o cuando ello pueda obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, a las investigaciones penales sobre la comisión de faltas o delitos, al desarrollo de funciones de control de la salud y del medio ambiente, a la verificación de infracciones administrativas, o cuando así lo disponga la ley.

a. Derecho de información

Como se vio anteriormente, el derecho de información consta descrito en el artículo 18 relativo al tratamiento de datos personales por el cual si el responsable del fichero

recoge datos de un titular debe cumplir con informar de forma detallada, sencilla, expresa, inequívoca y de manera previa sobre la finalidad para la cual sus datos personales serán tratados, destinatarios, la existencia del banco de datos en que se almacenarán, la identidad y domicilio del responsable del fichero o del encargado del tratamiento, entre otra información fundamental para que la persona pueda tomar una decisión informada sobre la entrega o tratamiento de sus datos personales.

b. Derecho de acceso

El derecho de acceso está presente en la Ley 28237, 31 de mayo de 2004, Código Procesal Constitucional que en su artículo 61 indica que mediante el proceso de *habeas data* se puede acceder a información que obre en poder de cualquier entidad pública, ya se trate de la que generen, produzcan, procesen o posean, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que la administración pública tenga en su poder, cualquiera que sea la forma de expresión, ya sea gráfica, sonora, visual, electromagnética o que obre en cualquier otro tipo de soporte material. Así como, conocer datos personales para ejercer otros derechos (ARCO) respecto de ficheros públicos y también privados.

Asimismo, el artículo 63 señala que, respecto de la ejecución anticipada de oficio o a pedido de la parte reclamante, en cualquier etapa del procedimiento y antes de dictar sentencia, el juez está autorizado para requerir al demandado que posee, administra o maneja el archivo, registro o banco de datos, la remisión de la información concerniente al reclamante; así como solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime conveniente. En este caso, el derecho de acceso lo ejerce un titular mediante una acción específica de ejecución anticipada.

Por su parte, el artículo 19 de la Ley de Protección de Datos Personales señala que el derecho de acceso permite al titular de datos personales el derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos.

c. Derecho de rectificación

Se infiere el derecho de rectificación en el numeral 2 del artículo 61 de Código Procesal Constitucional de 2004 cuando fija que el titular del dato podrá conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros.

Por su parte, el artículo 20 de la Ley de Protección de Datos Personales señala el derecho del titular de solicitar la actualización, inclusión, rectificación y supresión de sus datos personales, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando

hubiera vencido el plazo establecido para su tratamiento. Si sus datos personales hubieran sido transferidos previamente, el encargado del banco de datos personales debe comunicar la actualización, inclusión, rectificación o supresión a quienes se hayan transferido, en el caso de que se mantenga el tratamiento por este último, quien debe también proceder a la actualización, inclusión, rectificación o supresión, según corresponda. Durante el proceso de actualización, inclusión, rectificación o supresión de datos personales, el encargado del banco de datos personales dispone su bloqueo, quedando impedido de permitir que terceros accedan a ellos. Dicho bloqueo no es aplicable a las entidades públicas que requieren de tal información para el adecuado ejercicio de sus competencias; según la ley, estas deben informar que se encuentra en trámite cualquiera de los mencionados procesos.

d. Derecho de oposición

El artículo 22 de la Ley de Protección de Datos Personales hace mención a este derecho que no aparece reconocido en su antecesora el Código Procesal Constitucional de 2004. Dicho derecho señala que siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En caso de oposición justificada, el titular o el encargado del banco de datos personales, según corresponda, debe proceder a su supresión, conforme a ley. Llama la atención la precisión respecto del consentimiento, puesto que este, conforme se señaló previamente, puede revocarse en cualquier momento, de acuerdo con lo señalado en el numeral 7 del artículo 13, para lo cual la única limitación es observar en efecto, los mismos requisitos que con ocasión preste su otorgamiento.

e. Derecho de cancelación

El artículo 20 de la Ley de Protección de Datos Personales señala el derecho de supresión, término similar por el cual el titular de los datos personales tiene derecho a la supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento. Si sus datos personales hubieran sido transferidos previamente, el encargado del banco de datos personales debe comunicar la supresión a quienes se hayan transferido, en el caso de que se mantenga el tratamiento por este último, quien debe también proceder la supresión, según corresponda. Durante la ejecución de este proceso puede disponerse de un proceso de bloqueo por el cual los terceros están impedidos de acceder a ellos hasta su cancelación.

f. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

Asimismo, la misma Ley de Protección de Datos Personales señala con el nombre de derecho, al tratamiento objetivo recogido en el artículo 23 el derecho del titular de datos personales de no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, sustentada únicamente en un tratamiento de datos personales destinado a evaluar determinados aspectos de su personalidad o conducta, salvo que ello ocurra en el marco de la negociación, celebración o ejecución de un

contrato o en los casos de evaluación con fines de incorporación a una entidad pública, de acuerdo con la ley, sin perjuicio de la posibilidad de defender su punto de vista, para salvaguardar su legítimo interés.

g. Derecho de consulta al registro general de protección de datos personales

El artículo 34 de la ley en análisis señala la creación de la Autoridad Nacional de Protección de Datos Personales, cuya finalidad es recibir el Registro Nacional de Protección de Datos Personales de los bancos de datos personales de administración pública o privada, así como los datos relativos a estos que sean necesarios para el ejercicio de los derechos que corresponden a los titulares de datos personales, conforme a lo dispuesto en esta ley y en su reglamento.

h. Derecho a indemnización por daños causados

En el artículo 25 de la Ley de Protección de Datos Personales consta el derecho a ser indemnizado, por el cual el titular de los datos personales afectado por la consecuencia del incumplimiento de la presente ley por el responsable o por el encargado del banco de datos personales o por terceros tiene derecho a obtener la indemnización correspondiente conforme a ley.

i. Derecho a la confidencialidad

El artículo 17 de la citada Ley de Protección de Datos Personales señala un contenido bastante completo del derecho a la confidencialidad de los datos personales, por el cual el titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones y únicamente puede ser relevado de la obligación de confidencialidad cuando: a) medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales; b) resolución judicial consentida o ejecutoriada; c) o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública; d) todo ello, sin perjuicio del derecho a guardar el secreto profesional.

j. Derecho al olvido digital

Si bien no consta en la normativa de protección de datos, la Dirección General de Protección de Datos Personales en Expediente 045-2015-JUS/DGPDP reconoce el derecho al olvido digital y sanciona a Google Inc., domiciliada en Estados Unidos, obligándole a desindexar información relacionada a un juicio penal cubierto por medios de comunicación, del que nunca se le encontró responsable. La Dirección General de Protección de Datos Personales consideró que Google Inc. estaba debidamente notificada y era plenamente obligada a respetar las leyes peruanas, incluso si era una empresa extranjera que no se encontraba domiciliada debido a que trataba datos personales de peruanos y era accesible desde Perú.[1290]

k. Derecho de impedir el suministro

[1290] Dirección General de Protección de Datos Personales de la República del Perú, "Expediente 045-2015-JUS/DGPDP".

Otros de los derechos que señala la Ley de Protección de Datos Personales es el reconocido en el artículo 21, el cual determina al titular de datos personales el derecho a impedir que sean suministrados sus datos personales, especialmente cuando ello afecte sus derechos fundamentales. El derecho a impedir el suministro no aplica para la relación entre el titular del banco de datos personales y el encargado del banco de datos personales para los efectos del tratamiento de estos. Se refiere a lo que en otras legislaciones se denomina cesión de datos personales.

l. Derecho a la tutela

Respecto del artículo 24 de la Ley de Protección de Datos del Perú, consta el derecho a la tutela, por el cual el titular o el encargado del banco de datos personales que deniegue al titular de los datos personales, total o parcialmente, el ejercicio de los derechos establecidos en esta ley, puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de *habeas data*.

m. Spam

Respecto de Spam, existe la Ley 28493, publicada en el Diario Oficial, El Peruano, 12 de abril del 2005, ley que sistematiza el Uso del Correo Electrónico Comercial No Solicitado (Spam), por el cual regula el envío de comunicaciones comerciales publicitarias o promocionales no solicitadas, realizadas por correo electrónico, sin perjuicio de la aplicación de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor. De tal manera, se establece al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi) como la autoridad competente para velar por el cumplimiento de la citada ley.

g) Procedimiento

Como se señaló anteriormente cuando se mencionó el derecho a la tutela, el artículo 24 de la Ley de Protección de Datos del Perú señala que el titular o el encargado del banco de datos personales que deniegue al titular de los mismos, total o parcialmente, el ejercicio de los derechos establecidos en esta ley, puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de *habeas data*.

Si el procedimiento por el que se opta es el de seguir la acción ante la Autoridad Nacional de Protección de Datos Personales deberá sujetarse a lo dispuesto en los artículos 219 y siguientes de la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces. La resolución de la Autoridad Nacional de Protección de Datos Personales agota la vía administrativa y habilita la imposición de las sanciones administrativas previstas en el artículo 39. El reglamento determina las instancias correspondientes. Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa.

h) Habeas data

Es una garantía constitucional que constituye una acción jurisdiccional que se sigue ante el Poder Judicial, por el cual y conforme el artículo 200 de la Constitución de la

República del Perú: "Garantías constitucionales: Son garantías constitucionales: [...] 3) La acción de hábeas data, que procede contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el Artículo 2, inciso 5) y 6) de la Constitución"[1291].

a. Sujeto activo

De conformidad con la expresión general, toda persona, recogida en el artículo 61 de la Ley 28237, de 31 de mayo de 2004, Código Procesal Constitucional; y tal como consta analizado respecto de los titulares del derecho fundamental a la protección de datos personales, son titulares activos de la acción de habeas data tanto la persona natural como la jurídica.

b. Sujetos pasivos u obligados

Al tenor de lo dispuesto en el artículo 61 del citado Código Procesal Constitucional, serán sujetos pasivos de la acción constitucional de *habeas data*, las entidades públicas o instituciones privadas que traten, generen, produzcan, procesen o posean información, asimismo aquellas instituciones privadas que brinden servicio o acceso a terceros.

Conforme el artículo 28 de la Ley de Protección de Datos Personales, tienen obligaciones los sujetos pasivos, los titulares de las bases de datos, los encargados de las bases de datos y los terceros.

c. Derechos tutelados por el habeas data

El mencionado artículo 61 del Código Procesal Constitucional delimita expresamente que los derechos protegidos por el *habeas data* constan reconocidos en los incisos 5) y 6) del artículo 2 de la Constitución. En consecuencia, toda persona puede acudir a dicho proceso para proteger o tutelar el derecho a solicitar información pública y el derecho a la protección de datos personales.

d. Procedencia del habeas data

El artículo 2 de la Ley 28237, 31 de mayo de 2004, Código Procesal Constitucional, señala que la procedencia de los procesos constitucionales de *habeas corpus*, amparo y *habeas data* opera cuando se amenace o viole los derechos constitucionales por acción u omisión de actos de cumplimiento obligatorio, por parte de cualquier autoridad, funcionario o persona. Cuando se invoque la amenaza de violación, esta debe ser cierta y de inminente realización. El proceso de cumplimiento procede para que se acate una norma legal o se ejecute un acto administrativo.

Figura en el artículo 5 del Código Procesal Constitucional las causales de improcedencia de los procesos constitucionales, entre las cuales se expone el *habeas data* y determina los siguientes casos: 1. Los hechos y el petitorio de la demanda no están referidos en forma directa al contenido constitucionalmente protegido del derecho invocado; 2. Existan vías procedimentales específicas, igualmente satisfactorias, para la protección del derecho constitucional amenazado o vulnerado, salvo cuando se trate del

[1291] Congreso de la República del Perú, "Perú: Constitución Política de 1993 con reformas hasta 2005".

proceso de *habeas corpus*; 3. El agraviado haya recurrido previamente a otro proceso judicial para pedir tutela respecto de su derecho constitucional; 4. No se hayan agotado las vías previas, salvo justamente el caso de daño inminente previsto para el caso del habeas data que en este único caso prevé la posibilidad de no agotar la vía; 5. Que a la presentación de la demanda ha cesado la amenaza o violación de un derecho constitucional o se ha convertido en irreparable; 6. Que se cuestione una resolución firme recaída en otro proceso constitucional o haya litispendencia; 7. Que se cuestionen las resoluciones definitivas del Consejo Nacional de la Magistratura en materia de destitución y ratificación de jueces y fiscales, siempre que dichas resoluciones hayan sido motivadas y dictadas con audiencia previa al interesado; 8. Que se cuestionen las resoluciones del Jurado Nacional de Elecciones en materia electoral, salvo cuando no sean de naturaleza jurisdiccional o cuando siendo jurisdiccionales violen la tutela procesal efectiva. Tampoco procede contra las resoluciones de la Oficina Nacional de Procesos Electorales y del Registro Nacional de Identificación y Estado Civil si pueden ser revisadas por el Jurado Nacional de Elecciones; 9. Se trate de conflictos entre entidades de derecho público interno. Los conflictos constitucionales surgidos entre dichas entidades, sean poderes del Estado, órganos de nivel o relevancia constitucional, gobiernos locales y regionales, serán resueltos por las vías procedimentales correspondientes; 10. Que ha vencido el plazo para interponer la demanda, con excepción del proceso de *habeas corpus*.

e. Procedimiento del habeas data

En el artículo 62 de la Ley 28237, 31 de mayo de 2004, Código Procesal Constitucional, consta expresamente la necesidad de agotamiento de vía, ya que establece como requisito especial de la demanda y para la procedencia del *habeas data* que el demandante previamente haya reclamado, por documento de fecha cierta, el respeto de los derechos a que se refiere el artículo anterior, y que el demandado se haya ratificado en su incumplimiento o no haya contestado dentro de los diez días útiles siguientes a la presentación de la solicitud tratándose del derecho reconocido por el artículo 2 inciso 5) de la Constitución, o dentro de los dos días si se trata del derecho reconocido por el artículo 2 inciso 6) de la ya mencionada Carta Magna.

De esa forma se establece el procedimiento para interponer esta acción constitucional; solo de forma excepcional se podrá prescindir de este requisito de agotamiento de vía, y esto cuando exista un inminente peligro de sufrir un daño irreparable que puede ser evitado con una intervención inmediata, situación que deberá ser acreditada por el demandante. Aparte de dicho requisito, no será necesario agotar la vía administrativa que pudiera existir; de esta manera, el titular, conforme se señaló en líneas precedentes, tiene la opción de iniciar una acción administrativa o una acción jurisdiccional constitucional, o incluso iniciar las dos de forma simultánea.

Asimismo, en su parte pertinente el artículo 15 del Código Procesal Constitucional admite la posibilidad de dictarse medidas cautelares por las cuales se puede suspender actos violatorios discutidos en procesos de amparo, *habeas data* y de cumplimiento. Para su expedición se exigirá apariencia del derecho, peligro en la demora y que el pedido cautelar sea adecuado para garantizar la eficacia de la pretensión. Se dictan sin conocimiento de la contraparte y la apelación solo es concedida sin efecto suspensivo. Su procedencia, trámite y ejecución dependen del contenido de la pretensión constitucional intentada y del aseguramiento de la decisión final. El juez al conceder la

medida atenderá al límite de irreversibilidad de la misma. De la solicitud se corre traslado por el término de tres días, acompañando copia certificada de la demanda y sus recaudos, así como de la resolución que la da por admitida, tramitando el incidente en cuerda separada, con intervención del Ministerio Público. Con la contestación expresa o ficta la Corte Superior resolverá dentro del plazo de tres días bajo responsabilidad, salvo que se haya formulado solicitud de informe oral, en cuyo caso el plazo se computará a partir de la fecha de su realización. La resolución que dicta la Corte será recurrible con efecto suspensivo ante la Corte Suprema de Justicia de la República, la cual resolverá en el plazo de diez días de elevados los autos, bajo responsabilidad.

Respecto de la resolución de segundo grado consta en el artículo 18 del Código Procesal Constitucional el *recurso de agravio constitucional*, que declarará infundada o improcedente la demanda, dentro del plazo de diez días contados desde el día siguiente de notificada la resolución. Concedido el recurso, el Presidente de la Sala remite al Tribunal Constitucional el expediente dentro del plazo máximo de tres días, más el término de la distancia, bajo responsabilidad.

Acerca de la resolución que deniega el recurso de agravio constitucional procede el recurso de queja, contemplado en el artículo 19 del Código Procesal Constitucional, el cual se interpone ante el Tribunal Constitucional dentro del plazo de cinco días siguientes a la notificación de la denegatoria. Al escrito que contiene el recurso y su fundamentación, se anexa copia de la resolución recurrida y de la denegatoria, certificada por abogado, salvo el caso del proceso de *habeas corpus*. El recurso será resuelto dentro de los diez días de recibido, sin dar lugar a trámite. Si el Tribunal Constitucional declara fundada la queja, conoce también el recurso de agravio constitucional, ordenando al juez superior el envío del expediente dentro del tercer día de oficiado, bajo responsabilidad.

El artículo 20 de la citada ley señala que el Tribunal Constitucional deberá pronunciarse respecto de las resoluciones denegatorias de los procesos de amparo, *habeas data* y de cumplimiento, de los procesos de *habeas corpus* dentro de los treinta días de interpuesto.

Finalmente, el artículo 64 de la citada ley declara que tratándose de la protección de datos personales, podrán acumularse las pretensiones de acceder y conocer informaciones de una persona, con las de actualizar, rectificar, incluir, suprimir o impedir que se suministren datos o informaciones.

i) Institucionalidad de protección

La Ley de Protección de Datos Personales en el artículo 32 señala como órgano competente para proteger este derecho fundamental a la Autoridad Nacional de Protección de Datos Personales dependiente de la Dirección Nacional de Justicia del Ministerio de Justicia.[1292] Goza de potestad sancionadora, así como de potestad coactiva. La Autoridad Nacional de Protección de Datos Personales debe presentar periódicamente un informe sobre sus actividades al Ministro de Justicia.

[1292] Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales | Ministerio de Justicia y Derechos Humanos del Perú, Sitio web institucional de la Autoridad Nacional de Protección de Datos Personales dependiente de la Dirección Nacional de Justicia del Ministerio de Justicia.

j) Régimen sancionador

El Título VII sobre Infracciones y Sanciones Administrativas de la Ley de Protección de Datos Personales expresa en los artículos 37 a 40 sobre el procedimiento sancionador, infracciones leves, graves y muy graves, sanciones administrativas y multas coercitivas, respectivamente. Respecto al procedimiento sancionador, este se inicia de oficio, por parte de la Autoridad Nacional de Protección de Datos Personales o por denuncia de parte, ante la presunta comisión de actos contrarios a lo dispuesto en la presente ley o en su reglamento. Las resoluciones de la Autoridad Nacional de Protección de Datos Personales agotan la vía administrativa; contra las resoluciones de dicha autoridad procede la acción contencioso-administrativa. Respecto de la calificación, la graduación del monto de las multas, el procedimiento para su aplicación y otras tipificaciones constan descritas en el reglamento a la ley.

Respecto de las sanciones civiles, consta lo dispuesto en el artículo 39 de la citada ley que admite que la imposición de la multa se efectúa sin perjuicio de las sanciones disciplinarias sobre el personal de las entidades públicas en los casos de bancos de datos personales de administración pública, así como de la indemnización por daños y perjuicios y de las sanciones penales a que hubiera lugar.

k) Transferencia internacional de datos

Respecto de la transferencia internacional de datos personales, el artículo 2 de la ley de la materia señala entre las definiciones el de Flujo transfronterizo de datos personales, entendido como aquella transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los mismos, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban. Además, el mismo artículo fija en el numeral 10, que el nivel suficiente de protección para los datos personales abarca por lo menos la consignación y el respeto de los principios rectores de la ley citada, así como medidas técnicas de seguridad y confidencialidad. Finalmente, el artículo 15 de la ley determina que el titular y el encargado del banco de datos personales deben realizar el flujo transfronterizo de datos personales solo si el país destinatario mantiene niveles de protección adecuados conforme a la presente ley.

2.6 Argentina (1994)

La Constitución de la Nación Argentina el 22 de agosto de 1994 es reformada y el *habeas data* es incluido como acción y como subtipo de amparo, en el párrafo 3° del artículo 43 que dice: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística"[1293].

[1293] Convención Nacional Constituyente, "Argentina: Constitución de 1994", *Political Database of the Americas*, 1994, accedido 29 de junio de 2017, http://pdba.georgetown.edu/Constitutions/Argentina/argen94.html.

Como normativa de aplicación nacional la Ley 16.986, Ley de Acción de Amparo de 1966,[1294] desarrolla el contenido procedimental de esta garantía constitucional, añadiéndose que cada provincia ha desarrollado normativa específica sobre la materia.

La norma constitucional citada, consagra al *habeas data* como acción constitucional para garantizar al ciudadano su privacidad e intimidad que eran los derechos resultantes o reconocidos en los artículos 18 (inviolabilidad del domicilio y la correspondencia)[1295] y 19 (privacidad e intimidad)[1296] de la citada Constitución. Fernández Delpech señala que "se discute en doctrina si el derecho a la intimidad y a la protección de datos personales se encontraba incorporado en la Constitución Nacional de 1853-1860 por imperio de los arts. 18 y 19, pero lo cierto es que con la Reforma Constitucional de 1994, al incorporarse a la misma el art. 43, en su tercer párrafo se introdujo la acción de hábeas data, dando así cabida constitucional al derecho a la intimidad y a la protección de los datos personales [...] El término hábeas data significa «tiene sus datos» y lo que tiende a proteger es la privacidad o intimidad de las personas"[1297]. De lo citado se desprende que, aunque de la redacción de la norma se comprende que el *habeas data* protege los datos personales, aún no estaba clara la autonomía e independencia del derecho a la protección de datos personales.

Dos años después se aprobó la ley de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos, la Ley 24766.[1298] Ahora bien, es la "Corte Suprema de Justicia de la Nación la que ha otorgado una especial amplitud al instituto y lo han llevado a exceder considerablemente los contornos establecidos,[1299] llevando al Congreso Nacional a dictar la Ley 25.326 de Protección de los Datos

[1294] Presidencia de la República Argentina, "Ley 16.986, Ley de Acción de Amparo", *Dirección Nacional del Sistema Argentino de Información Jurídica, SAIJ.*, 1966, accedido 7 de julio de 2017, http://www.saij.gob.ar/16986-nacional-ley-accion-amparo-lns0001314-1966-10-18/123456789-0abc-defg-g41-31000scanyel.

[1295] Convención Nacional Constituyente, "Argentina: Constitución de 1994": "Artículo 18- Ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso, ni juzgado por comisiones especiales, o sacado de los jueces designados por la ley antes del hecho de la causa. Nadie puede ser obligado a declarar contra sí mismo; ni arrestado sino en virtud de orden escrita de autoridad competente. Es inviolable la defensa en juicio de la persona y de los derechos. El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación. Quedan abolidos para siempre la pena de muerte por causas políticas, toda especie de tormento y los azotes. Las cárceles de la Nación serán sanas y limpias, para seguridad y no para castigo de los reos detenidos en ellas, y toda medida que a pretexto de precaución conduzca a mortificarlos más allá de lo que aquella exija, hará responsable al juez que la autorice".

[1296] Ibíd. "Artículo 19- Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe".

[1297] H. FERNÁNDEZ DELPECH, *Manual de derecho informático* (Buenos Aires: Abeledo Perrot, 2014), 331.

[1298] Senado y Cámara de Diputados de la Nación Argentina, "Ley 24766, Ley de Confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos", 1996, accedido 8 de julio de 2017, http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41094/norma.htm.

[1299] E. C. PÉREZ-LUÑO ROBLEDO, *El procedimiento de habeas data el derecho procesal ante las nuevas tecnologías*, Dykinson, S.l., 2017, 138, accedido 8 de julio de 2017, http://www.jstor.org/stable/10.2307/j.ctt1qqhfj6.

Personales, 2 de noviembre de 2000[1300] con la cual el derecho a la protección de datos aparece diferenciado, aunque limitado al acceso, pues el artículo 1 de la citada ley señala expresamente que:

> Artículo 1. La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.[1301]

Posteriormente, el Congreso de la República argentina reformó la versión original mediante Ley 26.343 de Modificación de la Ley de Protección de los Datos Personales, 9 de enero de 2008.[1302]

Asimismo, en el año 2001 la Presidencia de la República argentina dictó el Decreto 1.558/2001 que reglamenta la Ley 25326, sobre Protección de los Datos Personales,[1303] con la cual se intenta zanjar parte de esta discusión al reconocer que no se necesita del carácter informativo del dato pues no solo deben ser registradas las bases privadas destinadas a proveer información, sino todas independientemente del carácter informativo, excepto únicamente las personales domésticas. Para el 13 de agosto de 2010, mediante el Decreto Nacional 1.160/2010 se modificó el Anexo I del Decreto Reglamentario 1.558/2001.[1304]

Destaca en la normativa de la Provincia de Buenos Aires: la Constitución de la Provincia de Buenos Aires de 1994,[1305] la Ley de Amparo de la provincia de Buenos Aires de 2009,[1306] y de la Legislatura de la Provincia de Buenos Aires que para

---

[1300] Congreso de la República Argentina, "Ley 25.326 de Protección de los Datos Personales", *Dirección Nacional del Sistema Argentino de Información Jurídica, SAIJ.*, 2000, 326, accedido 29 de junio de 2017, http://www.saij.gob.ar/25326-nacional-ley-proteccion-datos-personales-lns0004499-2000-10-04/123456789-0abc-defg-g99-44000scanyel.

[1301] Ibíd..

[1302] Congreso de la República Argentina, "Ley 26.343 de Modificación de la ley de Protección de los Datos Personales", *Dirección Nacional del Sistema Argentino de Información Jurídica, SAIJ.*, 2008, 343, accedido 29 junio 2017, en http://www.saij.gob.ar/26343-nacional-modificacion-ley-proteccion-datos-personales-lnn0029629-2007-12-12/123456789-0abc-defg-g92-69200ncanyel?

[1303] Presidencia de la República Argentina, "Decreto 1.558/2001 Reglamentario de la ley 25326, sobre Protección de los Datos Personales", *Dirección Nacional del Sistema Argentino de Información Jurídica, SAIJ.*, 2001, accedido 29 de junio de 2017, http://www.saij.gob.ar/1558-nacional-decreto-reglamentario-ley-25326-sobre-proteccion-datos-personales-dn20010001558-2001-11-29/123456789-0abc-855-1000-1002soterced?

[1304] Presidencia de la República Argentina, "Decreto Nacional 1.160/2010 se modifica el Anexo I del Decreto Reglamentario 1.558/2001", *Dirección Nacional del Sistema Argentino de Información Jurídica, SAIJ*, 2010, accedido 1 de julio de 2017, http://www.saij.gob.ar/1160-nacional-modificacion-anexo-decreto-reglamentario-1558-01-dn20100001160-2010-08-11/123456789-0abc-061-1000-0102soterced?q=%28numero-norma%3A1160%20%29&o=5&f=Total%7CTipo%20de%20Documento/Legislaci%F3n/Decreto%7CFecha%7COrganismo%7CPublicaci%F3n%7CTema%7CEstado%20de%20Vigencia%7CAutor%7CJurisdicci%F3n&t=16.

[1305] Convención Constituyente, "Constitución de la Provincia de Buenos Aires", 1994, accedido 7 de julio de 2017, http://www.infoleg.gob.ar/?page_id=173.

[1306] Senado y Cámara de Diputados de la Provincia de Buenos Aires, "Ley 13.928: Contenido de la ley de amparo en la Provincia de Buenos Aires", *Dirección Nacional del Sistema Argentino de Información Jurídica, SAIJ.*, 2009, 928, accedido 8 de julio de 2017, http://www.saij.gob.ar/santiago-jose-ramos-ley-

aplicación en dicha circunscripción territorial dictó la Ley 1.845 de Protección de Datos Personales el 3 de agosto de 2006.[1307]

Como legislación nacional, para agosto de 2014 se sancionó la Ley 26.951 que creó el Registro Nacional "No Llame",[1308] así como para enero de 2015 se dictó el Decreto 2501/14 que reglamenta la Ley 26.951 sobre Creación del Registro Nacional "No Llame"[1309], cuyo objetivo es establecer un fichero al que una persona natural o jurídica puede suscribirse para que manifieste su voluntad de no ser contactada por quienes publicitan, ofertan, venden o regalan bienes y servicios.

Finalmente, la Dirección Nacional de Protección de Datos Personales puede dictar resoluciones de aplicación general que completan la normativa nacional de protección de datos personales, en su carácter de autoridad de aplicación (art. 9 de la Ley 26.951).

De otro lado, la Ley 25.326 de Protección de los Datos Personales, 2 de noviembre de 2000, incorpora dos artículos en la Ley 11.179, Código Penal, 16 de enero de 1985.[1310]

13928-contenido-ley-amparo-provincia-buenos-aires-dacf090077-2009-10/123456789-0abc-defg7700-90fcanirtcod.

[1307] Legislatura de la Provincia de Buenos Aires, "Ley 1.845 de Protección de Datos Personales", *Dirección Nacional del Sistema Argentino de Información Jurídica, SAIJ*, 2006, accedido 29 de junio de 2017, http://www.saij.gob.ar/1845-local-ciudad-autonoma-buenos-aires-ley-proteccion-datos-personales-lpx0001845-2005-11-24/123456789-0abc-defg-548-1000xvorpyel?&o=6&f=Total%7CFecha/2005/11%7CEstado%20de%20Vigencia/Vigente%2C%20de%20alcance%20general%7CTema%5B5%2C1%5D%7COrganismo%5B5%2C1%5D%7CAutor%5B5%2C1%5D%7CJurisdicci%F3n/Local/Ciudad%20Aut%F3noma%20de%20Buenos%20Aires%7CTribunal%5B5%2C1%5D%7CPublicaci%F3n%5B5%2C1%5D%7CColecci%F3n%20tem%E1tica%5B5%2C1%5D%7CTipo%20de%20Documento/Legislaci%F3n/Ley&t=11.

[1308] Congreso de la República Argentina, "Ley 26.951, Creación del Registro Nacional «No Llame»", *Dirección Nacional del Sistema Argentino de Información Jurídica, SAIJ*, 2014, accedido 1 de julio de 2017, http://www.saij.gob.ar/26951-nacional-creacion-registro-nacional-llame-lns0005923-2014-07-02/123456789-0abc-defg-g32-95000scanyel?q=%28numero-norma%3A26951%20%29&o=0&f=Total%7CTipo%20de%20Documento/Legislaci%F3n%7CFecha%7COrganismo%7CPublicaci%F3n%7CTema%7CEstado%20de%20Vigencia%7CAutor%7CJurisdicci%F3n&t=1.

[1309] Presidencia de la República Argentina, "Decreto 2501/14 sobre Creación del Registro Nacional No Llame, que reglamenta la Ley 26.951", *Dirección Nacional del Sistema Argentino de Información Jurídica, SAIJ*, 2015, accedido 1 de julio de 2017, http://www.saij.gob.ar/2501-nacional-reglamentacion-ley-26951-sobre-creacion-registro-nacional-llame-dn20140002501-2014-12-17/123456789-0abc-105-2000-4102soterced.

[1310] "Artículo 117.- El acusado de injuria o calumnia quedará exento de pena si se retractare públicamente, antes de contestar la querella o en el acto de hacerlo. La retractación no importará para el acusado la aceptación de su culpabilidad.

2. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

3. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

4. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".

Artículo 157.- Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos". Congreso de la República Argentina, "Ley 11.179, Código Penal", Dirección Nacional del Sistema Argentino de Información Jurídica, SAIJ, 1985, accedido 3 de julio de 2017, http://www.saij.gob.ar/11179-nacional-codigo-penal-lns0002677-1984-12-21/123456789-0abc-defg-g77-62000scanyel?#I0157.

Recientemente, se ha dictado la Ley 27275, de Derecho de Acceso a la Información Pública, 29 de septiembre de 2016.[1311]

Finalmente, en la Decisión 2003/490/CE, 30 de junio de 2003, de la Comisión de la Unión Europea, se declaró a Argentina como país adecuado para el tratamiento de datos personales, es decir que cumple con lo dispuesto en la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Argentina fue el primer país latinoamericano en tener este reconocimiento,[1312] que fuera modificado en virtud de la sentencia Schrems para sustituir las disposiciones que limitaban las facultades de las autoridades nacionales de supervisión y ampliarlas; además se impone la obligación de comprobar periódicamente si la conclusión relativa a la adecuación del nivel de protección ofrecido por el tercer país en cuestión, aún está objetiva y jurídicamente justificada. A la luz de las conclusiones de la sentencia en lo que se refiere al acceso a los datos personales por parte de las autoridades públicas, también deberá hacerse un seguimiento de las normas y prácticas que regulen dicho acceso, a través de Decisión de Ejecución (UE) 2016/2295 de la Comisión, de 16 de diciembre de 2016, por la que se modifican las Decisiones 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE, 2011/61/UE, y las Decisiones de Ejecución 2012/484/UE y 2013/65/UE, relativas a la protección adecuada de los datos personales por determinados países, en aplicación del artículo 25, apartado 6, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.[1313]

Se analizará para efectos de la presente investigación la normativa de aplicación general, esto es la Ley 25.326 de Protección de Datos Personales (en adelante LPDP).

Mediante Decreto de Necesidad y Urgencia Nº 746/20171314 se añadió como función del Jefe de Gabinete de Ministros "32. Garantizar el efectivo ejercicio del derecho de acceso a la información pública y controlar la aplicación de la Ley N° 25.326 de Protección de los Datos Personales".

[1311] Congreso de la República Argentina, "Ley 27275, Derecho de Acceso a la Información Pública Objeto", *Boletín Oficial de la República Argentina*, 2016, accedido 3 de julio de 2017, https://www.boletinoficial.gob.ar/#!DetalleNorma/151503/20160929.

[1312] "Decisión 2003/490/CE, de 30 de junio de 2003, de la Comisión de la Unión Europea, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina (Texto pertinente a efectos del EEE)", *EUR-Lex - 32003D0490 - EN - EUR-Lex*, 2003, accedido 25 de agosto de 2017, http://eur-lex.europa.eu/legal-content/ES/TXT/?toc=OJ%3AL%3A2003%3A168%3ATOC&uri=uriserv%3AOJ.L_.2003.168.01.0019.01.SPA.

[1313] La Comisión Europea, "Decisión de Ejecución (UE) 2016/2295 de la Comisión, de 16 de diciembre de 2016, por la que se modifican las Decisiones 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE, 2011/61/UE, y las Decisiones de Ejecución 2012/484/UE y 2013/65/UE, relativas a la protección adecuada de los datos personales por determinados países, en aplicación del artículo 25, apartado 6, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo [notificada con el número C(2016) 8353] (Texto pertinente a efectos del EEE)", *EUR-Lex - 32016D2295 - EN - EUR-Lex*, accedido 25 de agosto de 2017, http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016D2295.

[1314] Presidencia de la Nación Argentina, Decreto de Necesidad y Urgencia Nº 746/2017, accedido el 27 de agosto de 2019, http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/279940/norma.htm

El Decreto Nº 899/20171315 determina en su artículo 29 que la Agencia de acceso a la información pública, es el órgano de control de la Ley nº 25.326, Ley de protección de datos personales.

Finalmente, por Decreto 685/2017[1316] se nombra al Director de la Agencia de Acceso a la Información pública, por 5 años, con rango y jerarquía de secretario, autoridad que conforme se señaló previamente asumen también las responsabilidades dispuestas en la Ley de Protección de Datos Personales.

De otro lado, el 25 de febrero de 2019 Argentina ratifica el Convenio Nº108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, adoptado en Estrasburgo, y el Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos adoptado en Estrasburgo, el 8 de noviembre de 2001. Dicha normativa entró en vigencia el 01 de junio de 2019, de esta forma Argentina es el tercer país latinoamericano en ratificar este Convenio.

Desde el 2016 y con la entrada en vigencia en 2018 del RGPD, Argentina ha iniciado un proceso de reforma a la Ley No. 25.326, Ley de Protección de Datos Personales. El 18 de septiembre de 2018 la Presidencia de la Nación Argentina remite un proyecto de ley Congreso Nacional[1317] para que someter a su consideración. El texto del Proyecto de Ley[1318] en líneas generales se alinea al modelo europeo por lo que incluye nuevas categorías de datos como los genéticos y biométricos; limita los titulares de datos personales únicamente a personas físicas; acoge la figura del oficial de protección de datos, para el caso de que datos personales sensibles, de grandes cantidades de datos y del Estado; establece estándares para la legalidad del tratamiento de datos personales; incluye derechos adicionales como el derecho restringir el tratamiento de sus datos personales y el de portabilidad, elimina los requisitos para registrar bases de datos, establece la creación de una entidad autónoma de protección de datos.

Algunos activistas han cuestionado la falta de participación de la sociedad civil en el proceso de elaboración del anteproyecto, y además de varias críticas por incorporar de manera general la excepción de seguridad nacional y de interés legítimo como habilitantes para el procesamiento de datos personales sin necesidad de consentimiento, también se cuestiona la incorporación la disociación de datos y la figura de “fuentes de

[1315] Presidencia de la Nación Argentina, Decreto Nº 899/2017, accedido el 27 de agosto de 2019, http://servicios.infoleg.gob.ar/infolegInternet/anexos/285000-289999/285903/norma.htm

[1316] Presidencia de la Nación Argentina, Decreto 685/2017, accedido el 27 de agosto de 2019, https://www.argentina.gob.ar/normativa/nacional/decreto-685-2017-278734/texto

[1317] Presidencia de la Nación Argentina, Mensaje 147/2018 Proyecto de Ley de Protección de Datos Personales. Versión enviada por el Poder Ejecutivo Nacional al Congreso para someter a su consideración, accedido el 27 de agosto de 2019, https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales

[1318] Presidencia de la Nación Argentina, Proyecto de Ley de Datos Personales, accedido el 27 de agosto de 2019, https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf

acceso público irrestricto", la primera por no estar comprobada su efectividad, la segunda, por no especificar cuál es el alcance de la figura.[1319]

a) Ámbito: Registros o ficheros públicos y privados

Respecto del ámbito de protección de los datos personales, por expresión del artículo 1 de la LPDP, cuyo objeto es la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos o privados.

Asimismo, el artículo 22 LPDP determina que las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial. De esta manera, se visualiza que los ficheros regentados por entidades públicas son parte de ámbito de protección.

Por cuanto Argentina mantiene un sistema federado, se aclara que las normas de la presente ley son de orden público y de aplicación en lo pertinente en todo el territorio nacional. Estas son aquellas contenidas en los capítulos I (relativo a las disposiciones generales), II (referente a principios generales relativos a la protección de datos), III (sobre derechos de los titulares de datos) y IV (respecto a usuarios y responsables de archivos, registros y bancos de datos) y el artículo 32 que incorpora reformas al Código Penal vigente (art. 44, LPDP).

Acerca del resto de normas que no han sido citadas, el mencionado artículo 44 invita a las provincias a adherir las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional. Además, aclara que la jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional.

b) Naturaleza del dato

La norma constitucional que consagra el amparo (*habeas data*), artículo 43, hace referencia a *datos que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes*. Si bien esta redacción causó en determinado momento dificultades para reconocer el carácter informativo del dato a tal punto que incluso se considera como presupuesto indispensable para la procedencia de la acción. Ahora bien, es mediante la Ley de Protección de Datos, Ley 25.326 que se aclara el concepto de datos y aunque aún varios autores señalan la necesidad de este carácter informativo, la entrada en vigencia del Decreto 1.558/2001 soluciona cualquier discrepancia, pues establece la obligatoriedad de registrar todo tipo de bases privadas sin importar si están o no destinadas a proveer informes por su potencialidad de serlo, excepto aquellas conocidas como personales (domésticas).

[1319] G. PISANU, Lo bueno, lo malo y lo mejorable: Nuevo proyecto de ley de protección de datos en Argentina, Accesnow, accedido 27 de agosto de 2019 https://www.accessnow.org/lo-bueno-lo-malo-y-lo-mejorable-nuevo-proyecto-de-ley-de-proteccion-de-datos-en-argentina/

No obstante, las dudas se solucionan al comprender el alcance de la definición de dato que consta en el artículo 2, LPDP, siendo aquella información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o *determinables*. Al mencionar información de cualquier tipo que no identifiquen, pero que puedan llegar a identificar, se comprende que aquella que incluso no tenga un carácter informativo en esencia, puede llegar a tenerlo, una vez que ha sido tratada por los actuales sistemas automatizados, por ejemplo los de minería de datos, que permiten incluso establecer perfiles completos de la personalidad de un individuo.

Por su parte, la clasificación de los datos reconoce a los datos sensibles, datos informatizados, datos de salud, relativos a antecedentes penales o contravencionales y, además, se desarrolla los conceptos de archivos, registros o bancos de datos:

Datos sensibles: Serán considerados datos sensibles, aquellos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual (art. 2, LPDP). Ninguna persona puede ser obligada a proporcionarlos y solo pueden ser recolectados y ser objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. Y queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros (art. 7, LPDP).

Datos relativos a antecedentes penales o contravencionales: Solo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas (núm. 4, art. 2, LPDP).

Datos de salud: Serán aquellos relativos a la salud física o mental de los pacientes que acudan a los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud que estén o hubieren estado bajo tratamiento de aquellos, respetando los principios del secreto profesional (art. 8, LPDP).

Datos informatizados: Serán aquellos datos personales sometidos al tratamiento o procesamiento electrónico o automatizado (art. 2, LPDP).

Archivos, registros o bancos de datos con fines de publicidad: En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando estos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento (art. 27, numeral 1, LPDP).

Archivos, registros o bancos de datos relativos a encuestas: No se considerarán datos recogidos aquellos que no puedan atribuirse a una persona determinada o determinable, por lo que las normas de la LPDP no se aplicarán a encuestas de opinión, mediciones y estadísticas, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas (art. 28, LPDP).

Bancos de datos destinados a prestar servicios de información crediticia: La Ley 26.343, de modificación de la Ley de Protección de los Datos Personales de enero de 2008, incorpora en el artículo 47 de la Ley 25.326 un texto relativo a los bancos de datos destinados a prestar servicios de información crediticia, por el cual se deberá eliminar y omitir el asiento en el futuro de todo dato referido a obligaciones y calificaciones asociadas de las personas físicas y jurídicas, cuyas obligaciones comerciales se hubieran constituido en mora, o cuyas obligaciones financieras hubieran sido clasificadas con categoría 2, 3, 4 o 5, según normativas del Banco Central de la República Argentina. En ambos casos durante el período comprendido entre el 1 de enero del año 2000 y el 10 de diciembre de 2003, siempre y cuando esas deudas hubieran sido canceladas o regularizadas al momento de entrada en vigencia de la presente ley o lo sean dentro de los 180 días posteriores a la misma. La suscripción de un plan de pagos por parte del deudor, o la homologación del acuerdo preventivo o del acuerdo preventivo extrajudicial importará la regularización de la deuda, a los fines de esta ley.

Respecto de los soportes o formas se considera al archivo, registro, base o banco de datos de forma indistinta ya que todos estos términos designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso (art. 2, LPDP). Esta amplitud de la redacción da cuenta que se incluye en el ámbito de protección los soportes físicos y los digitales.

Por tratamiento de datos se considera a las operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relación, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros por medio de comunicaciones, consultas, interconexiones o transferencias (art. 2, LPDP).

Otro de los procesos de datos será la disociación, por el que todo tratamiento de datos personales se establecerá de manera que la información obtenida no pueda asociarse a persona determinada o determinable (art. 2, LPDP).

Finalmente, como se señaló en líneas precedentes, existía una vieja discusión respecto de si estaban o no bajo la égida de la ley los datos personales contenidos en archivos que *no* generan informes para terceros dado que el artículo 43 de la Constitución señalaba que solo se protegía bajo la acción de amparo: los bancos de datos privados cuya finalidad fuera la de proveer informes. Esta discusión se zanjó cuando el artículo 1 del Decreto 1558/2001 determinó que en el concepto de "archivos, registros, bases o bancos de datos privados destinados a dar informes se comprenden aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito". De tal forma que solo quedarían por fuera de la regulación aquellas bases consideradas como personales domésticas porque se entiende que todas las demás proveen o pueden llegar a proveer informes, aunque no hayan sido facilitadas a terceros puesto que se protege la simple potencialidad de que así sea.

c) Sujeto activo

Tanto los artículos 1 y el 2, LPDP, señalan que será titular de los datos toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

En el artículo 14, LPDP, consta descrito que les corresponderá a los sucesores universales la titularidad del derecho de acceso en el caso de datos de personas fallecidas.

d) Sujeto pasivo

Tal como señala el artículo 2, LPDP, el *responsable de archivo*, registro, base o banco de datos será la persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

Asimismo, el citado artículo menciona como *usuario de datos* a toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o mediante conexión con los mismos.

Por su parte el artículo 25, LPDP, señala que el tratamiento puede darse por cuenta de *terceros*, quienes no podrán aplicar o utilizar los datos con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación. Además, una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa y cuando razonablemente se presuma la posibilidad de ulteriores encargos, hasta por dos años.

Se describe como responsables de ficheros de información crediticia a los que realizan la prestación de servicios de información crediticia, por la cual solo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento. O aquellos relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés (art. 26, núm. 1 y 2, LPDP).

e) Objeto o bien jurídico

a. Derecho de información

En el artículo 13 del Capítulo III de los Derechos de los titulares de datos de la Ley de Protección de Datos Personales se señala que toda persona puede solicitar información al organismo de control relativo a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita.

Cabe recalcar que en este caso el derecho de información no se lo ejercita ante los titulares de las bases de datos sino que las peticiones deberán dirigirse al organismo de control que la tendrá registrada (art. 13, LPDP), por lo que pareciere que en este caso se ha nominado como derecho de información cuando pareciera que el derecho en cuestión es el de consulta.

Ahora bien, el derecho de acceso (art. 14, LPDP) permite al titular solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados se relaciona directamente con el derecho de información por lo que complementan respecto de a quién dirigirse en el ejercicio del derecho.

b. Autodeterminación informativa

El *habeas data* reconocido en la Constitución Federal argentina de 1994 se incluye como subtipo de amparo, que determina que toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad. Y en caso de falsedad o discriminación exigir la supresión, rectificación, confidencialidad o actualización (párr. 3 del art. 43). Ahora bien, el artículo 1 de la citada Ley de Protección de Datos Personales señala expresamente que tiene por objeto la protección integral de estos datos para garantizar el derecho al honor y a la intimidad de las personas, así como el acceso a la información que sobre las mismas se registre (*habeas data*), de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución nacional.

De esa manera, no se reconoce a la autodeterminación informativa sino únicamente a una de sus facetas la relativa a la posibilidad de accionar para decidir sobre los derechos de acceso, rectificación, confidencialidad y actualización; sin embargo, este derecho no es absoluto sino limitado a la necesidad de probar que los datos son falsos o por medio de ellos se produce discriminación en su contra. Asimismo, si bien el sistema descansa sobre el consentimiento en la entrega de los datos personales por parte de su titular, no es suficiente si es que no se puede revocarlo en cualquier momento, y en este caso el derecho de revocación solo consta expresamente establecido para el caso de las cesiones (núm. 2, art. 11, LPDP).

c. Necesidad de mandato legal para tratamiento sin autorización del titular

Conforme el literal b) del numeral 2 del artículo 5, el consentimiento del titular puede suplirse cuando se recaben en virtud de una obligación legal.

Con los ejemplos que se evidencian a continuación, se desprende la necesidad de existencia de una norma legal que permita captar datos personales sin autorización de su titular, pues en todos aquellos casos no descritos a continuación es indispensable el consentimiento del titular.

El artículo 23 por medio de sus numerales 1, 2 y 3 señala los datos que por ley quedan sujetos al régimen desarrollado en la Ley de Protección de Datos Personales materia de análisis. Estos son: a) aquellos datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos o tratamiento con fines de fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia para el estricto cumplimiento de sus misiones o para la represión de delitos; b) aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.

El régimen es especial porque se necesita de una categorización específica basada en la fiabilidad y, además, porque aquellos datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Asimismo, el artículo 26 —numerales 1 y 2, LPDP— señala que para la prestación de servicios de información crediticia solo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito o al cumplimiento o incumplimiento de obligaciones, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento. Pero además, el numeral 5 del citado artículo establece que la prestación de servicios de información crediticia no requerirá el consentimiento previo del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de esta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios. Es decir, es la presente Ley de Protección de Datos Personales la que determina un régimen de consentimiento y de relevo de este por medio de disposiciones legales como la antes analizada.

Y respecto de los datos sensibles solo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, conforme señala el artículo 7, LPDP.

Finalmente, el artículo 5 en el numeral 2 señala aquellos casos en los que no es necesario el consentimiento y que por estar determinado en esta ley es posible su recolección, estos son: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes.

d. Principios

i. Deber de información

El artículo 6 de la Ley de Protección de Datos Personales señala que cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara sobre: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga; d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. Es decir, de las condiciones básicas para el ejercicio de los derechos que permiten la efectiva vigencia de este derecho fundamental.

ii. Pertinencia

El principio de pertinencia, al igual que en otras legislaciones, se encuentra integrado al principio de calidad. Esto por cuanto los numerales 1 y 7 del artículo 4, LPDP, señalan que los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido; y en el caso de que estos hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados deberán ser destruidos.

iii. Calidad

El principio de calidad se encuentra ampliamente recogido en el artículo 4, LPDP, cuando además de establecer la obligatoriedad de que para efecto de su tratamiento los datos personales que se recojan o almacenen de modo que permita el ejercicio de derechos de acceso y por medios leales, deberán ser ciertos, adecuados, exactos, actualizados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido, así como tampoco utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención; y en caso de que estos hayan dejado de ser necesarios o pertinentes deberán ser eliminados. La obligación de controlar la exactitud, completitud y actualización de los datos es del titular de la base de datos de oficio, sin necesidad de petición del titular de los datos.

iv. Finalidad

Como consta en el artículo 4, LPDP, anteriormente analizado, el principio de finalidad se encuentra incluido dentro del principio de calidad de datos, ya que se determina que no podrá almacenarse información sin que previamente el titular conozca la finalidad del fichero. Además de que no podrá mantenerse el registro y tratarse si es que la finalidad ya no es necesaria o pertinente. También deberá informarse respecto de la finalidad de la cesión de los datos, artículo 11, numeral 1, LPDP. No se podrá utilizar datos personales para una finalidad distinta a la recogida. Y se podrá solicitar al órgano estatal de registro las bases incluidas en él y las finalidades de las recogidas de los datos, tal como consta en el artículo 13, LPDP.

En abundancia, el artículo 3 LPDP señala que los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

v. Seguridad

Acerca del régimen de seguridad de los datos personales, el numeral 1 del artículo 9, LPDP, señala que el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, para así evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Finalmente, el numeral 2 del citado artículo 9, LPDP, señala la prohibición de registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

vi. Consentimiento

Entretanto, el artículo 5, LPDP, señala que el tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el cual deberá constar por escrito o por otro medio que permita se le equipare de acuerdo con las circunstancias.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, con notificación previa al requerido de datos, de la información descrita en el artículo 6 de la presente ley.

Respecto de la cesión, el artículo 11, LPDP, señala que los datos personales objeto de tratamiento solo pueden ser cedidos con el consentimiento previo del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo; es decir, este consentimiento es previo e informado y revocable.

vii. Licitud

Existe un principio propio del derecho argentino denominado licitud, que consta en el capítulo II, denominado principios generales relativos a la protección de datos personales, en el artículo 3, LPDP, por el cual la formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y reglamento pertinente. Esta licitud también se verifica al establecer la obligación de que los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

viii. Principio de utilización no abusiva

Por cuanto el inciso 3 del artículo 4, LPDP, señala que los datos personales no podrán ser tratados con finalidades distintas o incompatibles que aquellas que motivaron su obtención, se comprende que se incorpora en la legislación argentina el principio de utilización no abusiva.

ix. Cesión

Consta en el artículo 11, LPDP, que es parte del capítulo de Principios generales relativos a la protección de datos personales el principio de cesión, mediante el cual los datos personales objeto de tratamiento solo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario, y con el consentimiento previo del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

a. Derecho de acceso

El artículo 14, LPDP, señala que el titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos o privados destinados a proveer informes.

Esta petición deberá ser satisfecha dentro de los diez días después de haber sido intimado fehacientemente el responsable de la base de datos. El derecho de acceso solo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.

El artículo 15, LPDP, señala que para que el derecho de acceso sea eficiente es necesario que la información se suministre en forma clara, exenta de codificaciones y, en su caso, acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. Además, es fundamental que se entregue información amplia sobre la totalidad del registro perteneciente al titular que solicita su acceso, aun cuando el requerimiento solo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado. Finalmente, la información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

El artículo 14 del Decreto 1558/2001 garantiza al titular o, en caso de personas fallecidas a sus herederos, la solicitud de información sin fórmulas específicas, de manera directa, presentándose el interesado ante el responsable o usuario del archivo, registro, base o banco de datos, o de manera indirecta, mediante una intimación fehaciente por medio escrito que deje constancia de su recepción.

El acceso podrá consistir en la mera consulta de los archivos por medio de la visualización, o en la indicación de los datos objeto de tratamiento por escrito, por medios electrónicos, telefónicos, de imagen u otro idóneo a tal fin; y de acuerdo con lo establecido por el decreto reglamentario, permitirá que el titular de los datos:

> Artículo 14 [...] El derecho de acceso permitirá:
> 1) Conozca si se encuentra o no en el archivo, registro, base o banco de datos.
> 2) Conozca todos los datos relativos a su persona que consten en el archivo.
> 3) Solicite información sobre las fuentes y los medios a través de los cuales se obtuvieron sus datos.
> 4) Solicite las finalidades para las que sus datos fueron recabados.
> 5) Conozca el destino previsto para sus datos.
> 6) Sepa si el archivo se encuentra registrado en el registro habilitado por la Dirección Nacional de Protección de Datos Personales.
> Ante el requerimiento del interesado y su opción en cuanto al medio preferido para conocer la respuesta, el responsable o usuario del banco de datos deberá proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.
> Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, el titular de los datos tendrá expedita la acción de protección de los datos personales o de hábeas data prevista en el Capítulo VII de la Ley y denunciar el hecho ante la Dirección Nacional de Protección de Datos Personales.[1320]

[1320] Presidencia de la República Argentina, "Decreto 1.558/2001 Reglamentario de la ley 25326, sobre Protección de los Datos Personales", *Dirección Nacional del Sistema Argentino de Información Jurídica, SAIJ*., 2001, accedido 29 de junio de 2017, http://www.saij.gob.ar/1558-nacional-decreto-reglamentario-

b. Derecho de rectificación y actualización

Los derechos de rectificación, actualización o supresión constan descritos en el artículo 16, LPDP; de tal forma que toda persona tiene derecho a que el responsable del fichero rectifique, actualice y, cuando corresponda, suprima o someta a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos a reclamo de su titular o cuando el responsable del fichero hubiese advertido del error o falsedad.

Respecto de la cesión o transferencia de datos, el responsable o usuario del banco de datos deberá notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.

Para que se produzca la rectificación es necesario un proceso de verificación y rectificación del error o falsedad de la información que se trate, por lo que el responsable o usuario del banco de datos deberá: o bien bloquear el archivo o consignar al proveedor que la información se encuentra sometida a revisión.

Finalmente, conforme señala el artículo 17, LPDP, existe la posibilidad que los responsables o usuarios de bancos de datos públicos puedan, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la nación, del orden y la seguridad pública, o de la protección de los derechos e intereses de terceros, se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas.

Conforme el artículo 19, LPDP, se rectificarán o suprimirán los datos personales inexactos o incompletos que obren en registros públicos o privados sin cargo alguno para el interesado.

c. Derecho de oposición

Si bien no consta descrito de forma expresa en el texto de la Ley de Protección de Datos Personales argentina, el derecho de oposición se infiere del contenido del principio de información cuando se señala que en el momento en que se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara sobre el carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga y las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos. Toda vez que el titular puede decidir oponerse a entregar sus datos personales en determinadas circunstancias.

---

ley-25326-sobre-proteccion-datos-personales-dn20010001558-2001-11-29/123456789-0abc-855-1000-1002soterced?

Adicionalmente, también se materializa en el contenido del numeral 1 del artículo 7, LPDP, cuando expresamente menciona que ninguna persona puede ser obligada a proporcionar datos sensibles.

d. Derecho de supresión

Por otro lado, los derechos de rectificación, actualización o supresión constan descritos en el artículo 16, LPDP. Específicamente sobre la supresión se aclara que esta no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos. De ese modo, los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables, o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.

El inciso 6 del artículo indicado señala que durante el proceso de verificación y rectificación del error o falsedad de la información, el responsable o usuario del banco de datos podrá bloquear el archivo, o notificar al proveedor de información, la circunstancia de que se encuentra sometida a revisión. De esta manera, se puede reconocer que dentro del derecho de cancelación se establece un derecho de bloqueo.

Se aclara que respecto de archivos de datos con fines promocionales, comerciales o publicitarios, el artículo 27 numeral 1 señala que el titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de estos bancos de datos.

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

El numeral 1 del artículo 20, LPDP, señala que las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado. De esta forma, se establece una limitación a las valoraciones producto de procesos automatizados debido a la posibilidad de que pudieran afectar derechos fundamentales. Llama la atención que la sanción a la existencia de actos que vayan en contra de esta disposición es la nulidad insanable, por lo tanto nulidad absoluta que no admite ratificación ni convalidación.

f. Derecho de consulta al registro general de protección de datos personales

El artículo 21, LPDP, recogido en el capítulo IV de usuarios y responsables de archivos, registros y bancos de datos determina que todo archivo, registro, base o banco de datos públicos y privados destinados a proporcionar informes debe inscribirse en el registro que al efecto habilite el organismo de control; y deberá comprender como mínimo la siguiente información: a) Nombre y domicilio del responsable; b) Características y finalidad del archivo; c) Naturaleza de los datos personales contenidos en cada archivo; d) Forma de recolección y actualización de datos; e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos; f) Modo de interrelacionar la información registrada; g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; h) Tiempo de conservación de los datos; i) Forma y

condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

Es importante mencionar que existe prohibición expresa respecto a que ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro. Por este motivo, el Decreto nacional 1.558/2001, Reglamentario de la Ley 25326, sobre Protección de los Datos Personales, 3 de diciembre de 2001, además de desarrollar las infracciones, las multas, las responsabilidades, señala la obligatoriedad de realizar inspecciones (art. 31, Decreto Nacional 1.558/2001).

Finalmente, el artículo 24 señala que los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal están obligados también a registrar.

g. Derecho a indemnización por daños causados

En el capítulo VI Sanciones, respecto de las sanciones administrativas consta el artículo 31 que menciona que sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos, es posible la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan; el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000) a cien mil pesos ($ 100.000), clausura o cancelación del archivo, registro o banco de datos. En otras palabras, se reconoce la norma general por la cual un mismo acto genera responsabilidades en distintos ámbitos, uno de ellos el civil que permite la reparación de daño mediante la indemnización económica.

h. Confidencialidad

Acerca de la confidencialidad, el numeral 1 del artículo 10, LPDP señala, que el responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

El numeral 2 de la citada norma señala que el obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

En el mismo sentido, el artículo 40 numeral 1 señala que los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere, salvo el caso en que se afecten las fuentes de información periodística.

i. Derecho al olvido digital

No se reconoce derecho al olvido digital en Argentina, ya que conforme la postura jurisprudencial descrita en el caso Rodríguez, María Belén c/ Google Inc. s/daños y perjuicios, Corte Suprema de Justicia de la Nación, 28 de octubre de 2014, se niega la petición de la interpuesta, entre otros, por motivos relacionados con la determinación de la responsabilidad subjetiva de los buscadores, la validez de las notificaciones judiciales y extrajudiciales y la libertad de expresión y censura previa. En especial, cabe

mencionar que se reconoce como mero intermediario al buscador conforme consta de la cita siguiente:

> 21. Que las consideraciones precedentes evidencian que la decisión apelada resulta infundada en este punto, en tanto considera directamente aplicable al caso la prohibición contenida en el art. 31 de la ley 11.723 sin reparar en que no se juzga aquí la responsabilidad que podría atribuirse a una página de Internet —por la indebida publicación o reproducción de imágenes— sino a un mero intermediario cuya única función es servir de enlace con aquélla.[1321]

j. Spam

El Spam no se encuentra reconocido legalmente en la República de Argentina. Ahora bien, en el año 2003, el Juzgado Civil y Comercial Federal nº 3, Secretaría nº 6 de la Capital Federal, dictó la primera medida cautelar contra el Spam.

En dicha sentencia se determinó que en aplicación de la Ley de Protección de Datos Personales, "el juez ordenó al demandado que, al menos mientras dure el litigio, se abstenga de seguir enviándonos mensajes de correo electrónico y que por ningún motivo transfiera o ceda a terceros ningún dato personal relacionado con nosotros, incluidas nuestras direcciones de correo electrónico"[1322].

g) Procedimiento

Conforme señala el artículo 14, LPDP, el titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales a los responsables de los bancos de datos públicos o privados.

Esta petición deberá ser satisfecha dentro de los diez días después de haber sido intimado fehacientemente el responsable de la base de datos. Si el responsable o usuario no proporciona la información solicitada dentro de los diez días corridos de haber sido requerido o si evacuado el informe, este se estimará insuficiente; se podrá presentar acción de protección de los datos personales o de *habeas data* legal.

En el mismo sentido y respecto de los derechos de rectificación, actualización o supresión descritos en el artículo 16, LPDP, el responsable deberá realizar todas las operaciones necesarias dentro del plazo máximo de cinco días hábiles de recibido el reclamo. El incumplimiento de esta obligación dentro del término, habilita a presentar la acción de protección de los datos personales o de *habeas data* legal.

Este tipo de acción se encuentra regulada en el capítulo VII, titulado Acción de Protección de los Datos Personales que regula la procedencia, la legitimación activa, la legitimación pasiva, la competencia, el procedimiento aplicable, los requisitos de la

[1321] Sala A de la Cámara Nacional de Apelaciones en lo Civil, "Sentencia No. 522/2014 en el caso: "Rodríguez, María Belén c/ Google Inc. s/daños y perjuicios", 2014, accedido 21 de junio de 2017, https://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verDocumentoById.html?idDocumento=7162581.

[1322] Juzgado Civil y Comercial Federal No. 3, Secretaría n.º 6 de la Capital Federal, Dr. Roberto Torti, "Tanús Gustavo Daniel y otro contra Cosa Carlo Alberto y otro. Expediente No. 1791-2003 - Sección No. 6", *Protección de Datos Personales - Argentina*, 2006, accedido 3 de julio de 2017, http://www.protecciondedatos.com.ar/.

demanda, el trámite, la confidencialidad del información, la contestación del informe, la ampliación de la demanda, la sentencia.

i. *Procedencia:* A fin de determinar cuándo procede la interposición de esta acción, el artículo 33, LPDP, realiza una enumeración de los casos en que se faculta su procedencia:

> Artículo 33.- 1. La acción de protección de los datos personales o de hábeas data procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.[1323]

Tres son los presupuestos fundamentales, esto es que la información se presuma falsa, inexacta o desactualizada, o su tratamiento prohibido de tal forma que las personas puedan ejercer su derecho a la autodeterminación informativa.

ii. *Legitimación activa:* Respecto de la legitimación activa de la acción de protección de datos personales o *habeas data* legal, el artículo 34, LPDP, señala que podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado de consanguinidad, por sí o por intermedio de apoderado.

En el caso de personas jurídicas, podrá ser interpuesta por sus representantes legales, o apoderados. Se recalca el papel del Defensor del Pueblo, quien a decir de la norma puede intervenir como coadyuvante.

iii. *Legitimación pasiva:* Respecto de la legitimación pasiva, es decir en contra de quien debe interponerse la acción, el artículo 35, LPDP, señala que deberá dirigirse en contra de los responsables y usuarios de bancos de datos públicos y de los privados destinados a proveer informes.

iv. *Competencia:* Cuando la competencia sea territorial, será competente para conocer de esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el cual el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor. Cuando la competencia sea federal procederá: cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales (art. 36, LPDP).

v. *Procedimiento aplicable:* Será aplicable el procedimiento señalado en la Ley de Protección de Datos personales, y además en aquellas que corresponda la

[1323] Senado y Cámara de Diputados de la Nación Argentina, Ley No. 25.326 'Ley de Protección de Datos Personales', de 04 de octubre de 2000", 2012, accedido 23 de junio de 2017, https://www.oas.org/juridico/pdfs/arg_ley25326.pdf

acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo (art. 37, LPDP).

vi. *Requisitos de la demanda:* Además de los requisitos básicos, es importante señalar sobre lo importante que el accionante alegue las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley (art. 38).

vii. *Trámite:* De ser admitida la acción, será el juez quien requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá, asimismo, solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente, todo ello dentro de un plazo de no más de cinco días hábiles, el cual podrá ser ampliado prudencialmente por el juez (art. 39, LPDP).

viii. *Confidencialidad de la información:* Solo podrán excusarse de cumplir con la remisión de la información si se afectan fuentes de información periodísticas; en los demás casos no se podrá alegar confidencialidad de la información (art. 40, LPDP).

ix. *Contestación del informe:* Los demandados podrán contestar el informe, entregando el archivo, registro o banco de datos, al cual se anexarán las razones por las que se incluyó la información cuestionada o aquellas por las que no se evacuó el pedido efectuado por el interesado (art. 41, LPDP).

x. *Ampliación de la demanda:* Ante la contestación del informe, descrita en el texto precedente, el actor podrá, en el término de tres días, ampliar el objeto de la demanda. De tal manera que pueda solicitar fundadamente la supresión, rectificación, confidencialidad o actualización de los datos personales falsos, erróneos, desactualizados o prohibidos de tratar. En el mismo acto se ofrecerá la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días (art. 42, LPDP). Se producirá una nueva contestación y prueba hasta cerrar el debate.

xi. *Sentencia:* Concluido el trámite se dictará sentencia que incluirá la determinación de la información a ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento y que deberá ser comunicada a la Dirección Nacional de Protección de Datos Personales. Se añade que el rechazo de la acción no faculta automáticamente a presumir responsabilidad.

h) Subtipo de amparo constitucional o habeas data constitucional

La acción de protección de datos personales o de *habeas data* se contempla en el artículo 43 de la Constitución de Argentina en las reformas introducidas en 1994; por su naturaleza tiene una doble dimensión: es una acción y un derecho al mismo tiempo.

Su contenido es más amplio que el de la acción judicial de protección de datos personales o *habeas data*, prevista en la Ley de Protección de Datos Personales, porque se relaciona directamente con la eficacia de los derechos constitucionales y no limitadamente con la falsedad, desactualización de unos datos personales, etc.

Además, existe una normativa de aplicación nacional: la Ley 16.986, Ley de Acción de Amparo de 1966;[1324] mientras que cada provincia tiene normativa específica, como por ejemplo, la Constitución de la Provincia de Buenos Aires de 1994[1325] y la Ley de Amparo de la provincia de Buenos Aires de 2009.[1326]

Por cuanto la identificación del contenido esencial necesita de normas generales y no sectoriales, así como tampoco puede analizarse normas cuya circunscripción de aplicación es limitada a un territorio específico de la nación, se analizará en este literal únicamente la norma de la Constitución de la Argentina y la ley nacional.

a. Sujeto activo

La norma constitucional señala expresamente a toda persona, natural y jurídica, respecto de este derecho en específico, toda vez que pueden ser invocados por un ente inmaterial, conforme el artículo 43 de la Constitución.

Asimismo, el artículo 5 la Ley de Acción de Amparo señala que podrá deducirse por toda persona individual o jurídica, por sí o por apoderados, por las asociaciones que sin revestir el carácter de personas jurídicas justificaren, mediante la exhibición de sus estatutos, que no contrarían una finalidad de bien público.

b. Sujetos pasivos u obligados

El artículo 43 de la Carta Magna argentina señala que deberá accionarse contra los responsables de los registros o bancos de datos públicos o de los privados destinados a proveer informes.

Por su parte, la Ley 16.986 señala en el artículo 1 que la acción de amparo se dirigirá en contra de autoridad pública que, en forma actual o inminente, lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, los derechos o garantías explícita o implícitamente reconocidas por la Constitución nacional.

c. Derechos tutelados por el habeas data

Como en el presente caso se trata de un subtipo de la acción de amparo, la norma constitucional al ser una garantía protege los derechos contemplados en el artículo 18 y 19 de la Carta Magna, esto es intimidad, privacidad, honor. Además, por referirse el

[1324] Presidencia de la República Argentina, "Ley 16.986, Ley de Acción de Amparo".
[1325] Convención Constituyente, "Constitución de la Provincia de Buenos Aires".
[1326] Senado y Cámara de Diputados de la Provincia de Buenos Aires, "Ley 13.928: Contenido de la ley de amparo en la Provincia de Buenos Aires", 928.

contenido del artículo 43 de la Constitución a que esta acción faculta a su titular a tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes se entiende que también está tutelado el derecho a la protección de datos personales, aunque en una versión limitada que apuntala al acceso más que un derecho de control sobre los datos personales de un titular.

d. Procedencia del habeas data

Como el *habeas data* constitucional es un subtipo de la acción de amparo, le es pertinente aquellos criterios de procedencia que definen a este tipo de acciones, esto es que toda persona natural o jurídica puede interponerlo cuando no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley (art. 43, Constitución argentina).

Pero además, los criterios propios de la acción de *habeas data* constitucional relativos a la necesidad de que la información personal conste en registros o bancos de datos públicos, o los privados destinados a proveer informes. Añadiendo que solo procede cuando los datos personales sean falsos o le generen a su titular discriminación (art. 43, Constitución argentina).

Asimismo, la Ley 16.986 señala en el artículo 2 que la acción de amparo no será admisible cuando: a) Existan recursos o remedios judiciales o administrativos que permitan obtener la protección del derecho o garantía constitucional de que se trate; b) El acto impugnado emanara de un órgano del Poder Judicial.

e. Procedimiento del habeas data

Respecto del procedimiento, es aplicable el establecido en la Ley 16.986, Ley de Acción de Amparo. Es decir, será competente para conocer de la acción de amparo el juez de Primera Instancia con jurisdicción en el lugar en el cual el acto se exteriorice o tuviere o pudiere tener efecto (art. 4).

La demanda deberá interponerse por escrito y principalmente contendrá: La relación circunstanciada de los extremos que hayan producido o estén en vías de producir la lesión del derecho o garantía constitucional (art. 6), la prueba instrumental de que disponga, o la individualizará si no se encontrase en su poder (art. 7).

Si la acción presentada fuera admisible, el juez requerirá a la autoridad que corresponda un informe circunstanciado acerca de los antecedentes y fundamento de la medida impugnada, que deberá ser evacuado dentro del plazo que fije. La omisión del pedido de informe es causa de nulidad del proceso. Una vez que el informe de la autoridad se haya entregado o haya vencido el plazo sin su presentación, se dictará sentencia fundada dentro de las 48 horas, concediendo o denegando el amparo (art. 8).

La sentencia que admita la acción deberá contener: a) La mención de la autoridad contra cuya resolución, acto u omisión se concede el amparo; b) La determinación de la

conducta a cumplir, con las especificaciones necesarias para su ejecución; c) El plazo para cumplimiento de lo resuelto (art. 12).

Solo serán apelables la sentencia definitiva, las resoluciones de inadmisibilidad manifiesta y las que dispongan medidas de no innovar o la suspensión de los efectos del acto impugnado. El recurso deberá interponerse dentro de 48 horas de notificada la resolución impugnada, debiendo denegarse o concederse en ambos efectos dentro de las 48 horas. En caso de concederse, se elevará el expediente al respectivo Tribunal de Alzada dentro de las 24 horas de ser concedido (art. 15).

i) Institucionalidad de protección

Conforme el artículo 29, LPDP, el órgano de control es la Dirección Nacional de Protección de Datos Personales,[1327] en el Ámbito de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos, como órgano de control de la citada ley.

Dicha dirección tendrá las funciones de asistir y asesorar a las personas para la defensa de los derechos de autodeterminación informativa y protección de datos personales, dictar las normas y reglamentaciones que desarrollen estos derechos; realizar un censo de archivos, registros o bancos de datos y mantener el registro permanente de los mismos; controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos; solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la ley; solicitar información a las entidades públicas; imponer sanciones administrativas de ser el caso y controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes.

j) Régimen sancionador

El artículo 31, LPDP, contenido en el capítulo VI sobre sanciones administrativas señala que los responsables de ficheros o los usuarios en el caso del cometimiento de infracciones serán responsables administrativa, civil y penalmente, con sanciones de apercibimiento, suspensión o multas.

El Decreto 1558, Reglamento LPDP, contiene la descripción de las acciones consideradas infracciones, las sanciones, los procedimientos para la aplicación de estas sanciones, las que deberán graduarse con relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

k) Transferencia internacional de datos

El artículo 12 LPDP, incluido en el capítulo de principios (no ha sido colocado en la parte pertinente para no desestructurar el análisis planteado en esta tesis), señala que respecto de la transferencia internacional está prohibida la transferencia de datos

[1327] "Datos Personales - Ministerio de Justicia y Derechos Humanos | Presidencia de la Nación", Sitio web institucional del Ministerio de Justicia y Derechos Humanos | Presidencia de la Nación- Datos Personales, accedido 2 de octubre de 2017, http://www.jus.gob.ar/datos-personales.aspx.

personales de cualquier tipo con países u organismos internacionales, o supranacionales, que no proporcionen niveles de protección adecuados.

Sin embargo, esta prohibición no es absoluta ya que existen casos que amerita el intercambio en razones de interés general o cuando la ley lo señale como: la colaboración judicial internacional; intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica; transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable; cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la república Argentina sea parte; cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

l) Códigos de conducta

Como parte de los principios que permiten la protección del objeto o bien jurídico del derecho a la protección de datos personales consta en los numerales 1 y 2 del artículo 30, LPDP, que las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.

Para que tengan efectividad se prevé que dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, el cual podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

m) Registro Nacional "No llame"

Mediante la Ley 26.951, 5 de agosto de 2014, se determina la creación de un registro nacional denominado "No llame", cuya finalidad es proteger a toda persona física o jurídica, titular de servicios de telefonía, en cualquiera de sus modalidades, de los abusos del procedimiento de contacto, publicidad, oferta, venta y regalo de bienes o servicios no solicitados (art. 1 de la citada ley). La inscripción y baja en el Registro es gratuita y deberá ser solicitada únicamente por el titular o usuario en cualquier momento y tendrá efectos inmediatos. Se crea, además, la Dirección Nacional de Protección de Datos Personales que impondrá sanciones administrativas en caso de infracciones a esta ley.

2.7 Nicaragua (1995)

La Constitución de Nicaragua, aprobada por la Asamblea Nacional Constituyente, el 19 de noviembre de 1986 y publicada en La Gaceta 94, del 30 de abril de 1987, contenía en el artículo 26 una referencia únicamente a la intimidad cuando señalaba que "Toda persona tiene derecho: 1. A su vida privada y la de su familia"[1328].

[1328] Asamblea Nacional Constituyente, "Nicaragua: Constitución de 1987", *Political Database of the Americas*, 1987, accedido 11 de mayo de 2017, http://pdba.georgetown.edu/Constitutions/Nica/nica87.html.

Posteriormente, la Ley 192, Ley de Reforma Parcial a la Constitución Política de la República de Nicaragua, aprobada el 1 de febrero de 1995 y publicada en La Gaceta, Diario Oficial 124 del, 4 de julio de 1995, reformó el artículo 26, estableciendo por primera vez[1329] el derecho a la protección de datos personales con el texto siguiente:

> Arto. 26. Toda persona tiene derecho: [...] 4) A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información.[1330]

Nuevamente el enfoque de la regulación es instrumental, medio para garantizar otros derechos de libertad. De forma específica intenta persuadir a la actuación estatal de la creación de ficheros con fines de hostigamiento político. Lo más sobresaliente, sin duda, es que, mediante un recurso de técnica legislativa, esto es, el uso de numerales, otorga al derecho a la protección de datos personales su carácter de derecho fundamental independiente, ya que lo consagra en el numeral 3 del citado artículo 26 de la Constitución. De esta forma, se distingue de otros derechos como el de la intimidad que consta en el numeral 1, el de la honra en el numeral 2 y el de la inviolabilidad del domicilio, en el numeral 4. Se materializa la autonomía del derecho a la protección de datos personales, especialmente respecto del derecho a la intimidad.

Tanto en la Constitución guatemalteca como en la nicaragüense se reconoce a la protección de datos, como derecho fundamental, aunque desde una visión sesgada pues solo esta sectorizada al control de las actuaciones estatales. Es decir, se adopta la postura europea de incorporación de un nuevo derecho, pero se lo hace con una perspectiva instrumental que busca la estabilidad democrática al garantizar a sus ciudadanos el respeto a su vida privada, y en consecuencia a su libertad de opinión, de expresión y de ideología, sobre todo, respecto de las transgresiones realizas por el Estado.

Tal como su predecesora, esa forma de reconocimiento del derecho corresponde a un abordaje de primera generación. Es recientemente que, mediante la Ley 854, Ley de Reforma Parcial a la Constitución Política de la República de Nicaragua, 29 de enero de 2014, publicado en la Gaceta 26, 10 de febrero de 2014,[1331] que se modificó nuevamente el artículo 26 y estableció el numeral 3 que señala:

> Artículo 26. Toda persona tiene derecho: [...] 3. A conocer toda información que sobre ella se haya registrado en las entidades de naturaleza privada y pública, así como el derecho de saber por qué y con qué finalidad se tiene esa información.[1332]

[1329] Al respecto, la Constitución de Nicaragua es de 1987 y la reforma que incluye la protección de datos personales como derecho es de 1995, por lo que conforme con Oscar Puccinelli y Nelson Remolina Angarita esta es la segunda Constitución que reconoce el derecho en Latinoamérica.

[1330] Asamblea Nacional de la República de Nicaragua, "Ley No. 192, Ley de Reforma Parcial a la Constitución Política de la República de Nicaragua", 1995, accedido 11 de mayo de 2017, http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/927804DC295D0AE5062573080056DA6D?OpenDocument.

[1331] Asamblea Nacional de la República de Nicaragua, "Ley No. 854, Ley de Reforma Parcial a la Constitución Política de la República de Nicaragua", 2014, accedido 11 de mayo de 2017, http://legislacion.asamblea.gob.ni/SILEG/Iniciativas.nsf/0/9e79461787f2f80f06257c1600609ea0/$FILE/29-01-2014%20Ley%20No.%20854%20Reformas%20Constitucionales.pdf.

[1332] "Constitución Política de la República de Nicaragua actualizada con las reformas introducidas por la Ley 854 de 2014, de 29 de Enero de 2014 - vLex Global", accedido 14 de mayo de 2017, https://app-vlex-

Es decir, el derecho a la protección de datos, a partir del 2014, no se limita a ficheros estatales, sino que protege los datos personales registrados en entidades privadas como públicas. Sin duda, un gran paso en el ámbito de aplicación del derecho que lo refuerza y completa el contenido esencial de este derecho en Nicaragua.

Respecto a la garantía constitucional del *habeas data*, esta aparece por primera vez en la Constitución de Nicaragua mediante las reformas introducidas por la Ley 854, de 29 de enero de 2014, con el texto siguiente:

> Artículo 45.- Las personas cuyos derechos constitucionales hayan sido violados o estén en peligro de serlo, pueden interponer el recurso de exhibición personal, de amparo, o de hábeas data, según el caso y de acuerdo con la Ley de Justicia Constitucional.[1333]

Llama la atención que su contenido está contemplado en el título IV de los derechos, deberes y garantías del pueblo nicaragüense, en el capítulo I de los derechos individuales. Pareciera que su concepción se ancla a las posiciones tradicionales que consideran al *habeas data* con una doble dimensión, es decir, como derecho fundamental y como recurso constitucional.

También, la misma ley reformatoria introduce en la Constitución Política de Nicaragua el título X sobre supremacía de la Constitución, su reforma y de las leyes constitucionales, en el capítulo II denominado "Control Constitucional", en específico el artículo 190, numeral 1, que establece la forma de ejercicio de esta garantía:

> Artículo 190.- Se establecen también los siguientes recursos y mecanismos de control constitucional: 1. El Recurso de *Habeas Data* como garantía de tutela de datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos, de naturaleza pública o privada, cuya publicidad constituya invasión a la privacidad personal y tenga relevancia con el tratamiento de datos sensibles de las personas en su ámbito íntimo y familiar. El Recurso de *Habeas Data* procede a favor de toda persona para saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales y su publicidad indebida.[1334]

Antes de la citada reforma a la Constitución de Nicaragua, el *habeas data* era únicamente un recurso legal constante en la Ley 831, Ley de Reforma y Adiciones a la Ley 49, Ley de Amparo, aprobada el 30 de enero del 2013, publicada en La Gaceta 29, del 14 de febrero del 2013, en cuyo artículo 5 consagraba el contenido y alcance del *habeas data*:

> Art. 5 bis. El Recurso de *Habeas Data* se crea como garantía de tutela de datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos, de naturaleza pública o privada, cuya publicidad constituya una invasión a la privacidad personal y tenga relevancia con el tratamiento de datos sensibles de las personas en su ámbito íntimo y familiar. El Recurso de *Habeas Data* procede a favor de toda persona

com.bibliotecavirtual.udla.edu.ec/?r=true#WW/search/*/constituci%C3%B3n+Nicaragua/WW/vid/514790313.

[1333] Ibíd.

[1334] Ibíd.

> para saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales y su publicidad indebida.[1335]

De lo transcrito, se colige que hasta antes de la reforma presentada en el 2014 el recurso de *habeas data* estaba solo consagrado a nivel legal, mientras que a partir de la mencionada reforma a la Carta Magna se lo comprende como un recurso y mecanismo de carácter constitucional.

Esa reforma introduce un total de 12 artículos que regulan el funcionamiento del *habeas data*, los cuales serán analizados en la medida en la que verifiquemos los elementos esenciales del derecho a la protección de datos en Nicaragua.

Antes de la consagración del *habeas data* como garantía constitucional, la Ley de Protección de Datos Personales, Ley 787-2012, aprobada el 21 de marzo del 2012, publicada en la Gaceta 61, del 29 de marzo del 2012,[1336] estableció su régimen legal. Esta norma se dictó entre dos y un año antes, respectivamente, de la consagración tanto del derecho fundamental a la protección de datos personales en las reformas introducidas en el año 2014, como del recurso constitucional de *habeas data* incorporado en la Constitución mediante las reformas del mismo año.

Asimismo, el Reglamento de la Ley 787-2012, Ley de Protección de Datos Personales, Decreto No. 36-2012, aprobado el 17 de octubre de 2012, publicado en la Gaceta 200, del 19 de octubre de 2012,[1337] contiene un régimen reglamentario de protección de los datos personales. Normativa sectorial, pues regula únicamente los datos personales que están en manos del Estado, consta en la Ley 621, aprobada el 16 de mayo del 2007, publicada en La Gaceta 118, del 22 de junio del 2007, Ley de Acceso a la Información Pública, la que incluyó la primera normativa relativa al *habeas data* en Nicaragua.

A continuación se realizará un análisis de aquellos elementos que nos permitirán construir un contenido esencial del derecho a la protección de datos personales en Nicaragua. El análisis se hará respecto de la normativa vigente, integrando los textos constitucionales y legales de carácter general vigentes a la fecha:

a) Ámbito: Registros o ficheros públicos

Originalmente, se reconoció a la protección de datos personales exclusivamente aplicable a registros o ficheros públicos en la Ley 192, Ley de Reforma Parcial a la Constitución Política de la República de Nicaragua, aprobada el 1 de febrero de 1995. Desde el año 2012 se estableció en la Ley 787-2012, Ley de Protección de Datos

[1335] Asamblea Nacional de Nicaragua, "Ley No. 831, Ley de Reforma y Adiciones a la Ley No. 49, Ley de Amparo", 2013, accedido 11 de mayo de 2017, http://legislacion.asamblea.gob.ni/normaweb.nsf/b92aaea87dac762406257265005d21f7/1b436b6b6399915d0625741700589df3?OpenDocument.

[1336] "Ley No. 787, Ley de Protección de Datos Personales de Nicaragua, de 29 de Marzo de 2012 - vLex Global", 2012, accedido 20 de mayo de 2017, https://app-vlex-com.bibliotecavirtual.udla.edu.ec/?r=true#WW/search/content_type:6/nicaragua+Ley+de+Protecci%C3%B3n+de+Datos+Personales%2C+Ley+No.+787%2C+aprobada+el+21+de+Marzo+del+2012%2C+publicada+en+la+Gaceta+No.+61+del+29+de+Marzo+del+2012/p2/WW/vid/645251929.

[1337] Presidencia de la República de Nicaragua, "Decreto No. 36-2012, Reglamento de la Ley No. 787 'Ley de Protección de Datos Personales de Nicaragua', de 19 de octubre de 2012 - vLex Global", 2012, accedido 20 de mayo de 2017, https://app-vlex-com.bibliotecavirtual.udla.edu.ec/?r=true#WW/vid/521277546.

Personales, es decir únicamente a nivel legal, que se protegerá a la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales tanto en ficheros de datos públicos como en aquellos privados conforme los artículos 1 y 2 de la Ley de Protección de Datos, en adelante Ley 787-2012. A partir de las reformas introducidas por la Ley 854, Ley de Reforma Parcial a la Constitución Política de la República de Nicaragua, de 29 de enero de 2014, el ámbito de aplicación son ficheros regentados, tanto por entidades estatales como por aquellas de carácter privado, con lo cual la protección tiene rango constitucional.

b) Naturaleza del dato

El vigente artículo 26 de la Constitución de Nicaragua, reformada en 2014, al referirse al derecho a conocer sobre lo que de una persona se haya registrado menciona el término *información*. En el artículo 190 de la mencionada Constitución, al consagrar el *habeas data* se señala que es una garantía que tutela datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos, de naturaleza pública o privada. Por su parte, la Ley de Reforma y Adiciones a la Ley 49, Ley de Amparo de 2013, señala en el artículo 5 bis, un texto idéntico al contemplado en la Constitución vigente, pero en el cual se añade que están dentro de la tutela también aquellos de naturaleza pública o privada. De esta forma, queda claro que el presupuesto de protección constituye, tanto la información como el dato personal, pues utiliza los términos como sinónimos.

En el mismo sentido, el artículo 84 de la Ley de Amparo señala que el recurso de *habeas data* faculta a toda persona al acceso a información personal que se encuentre en poder de cualquier entidad pública y privada de la cual generen, produzcan, procesen o posean información personal en expedientes, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier documento que tengan en su poder.

Ahora bien, respecto de la segunda parte del artículo 190 de la Constitución,[1338] la enunciación que se realiza sobre los tipos de soporte, lejos de favorecer la protección del derecho puede limitarla, tanto más que en la norma constitucional como en la legal se refiere únicamente a medios electrónicos y no a registros físicos. Sin embargo, esta afirmación se corrige tanto por el artículo 84 bis de la Ley de Amparo reformada, que señala que el *habeas data* faculta a exigir la oposición, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación y actualización, de datos personales sensibles independientemente de que sean físicos o electrónicos almacenados en ficheros de datos, o registro de entidades públicas o instituciones privadas. Asimismo, cuando el artículo 3 literal f) de la Ley de Protección de Datos en las definiciones señala expresamente que los datos personales informáticos son aquellos tratados a través de medios electrónicos o automatizados. En conclusión, se protege al dato tanto en el soporte físico como el electrónico. Y respecto al soporte electrónico del uso de la frase *otros medios técnicos*, se colige que la lista es meramente

[1338] "Artículo 190. Se establecen también los siguientes recursos y mecanismos de control constitucional: 1) El Recurso de *Habeas Data* como garantía de tutela de datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos, de naturaleza pública o privada, cuya publicidad constituya invasión a la privacidad personal y tenga relevancia con el tratamiento de datos sensibles de las personas en su ámbito íntimo y familiar. El Recurso de *Habeas Data* procede a favor de toda persona para saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales y su publicidad indebida". "Constitución Política de la República de Nicaragua actualizada con las reformas introducidas por la Ley 854 de 2014, de 29 de Enero de 2014 - vLex Global".

ejemplificativa, lo que al menos no limita en este aspecto la procedencia del *habeas data*.

La Ley 787-2012, Ley de Protección de Datos personales, en el artículo 3 relativo a las definiciones señala que "Datos personales: Es toda la información sobre una persona natural o jurídica que la identifica o la hace identificable"[1339], con lo cual el concepto de dato se alinea a lo que un estándar adecuado de protección plantea, puesto que de esta afirmación se colige que también se incluye al dato inocuo. La ley menciona, además, otras categorías como: a) datos personales informáticos, haciendo alusión a aquellos que han sido tratados por medios electrónicos o automatizados (arts. 3 y 8); b) datos personales sensibles, los que revelan origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas, económico-financieros; así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación.

Esos datos solo pueden ser obtenidos y tratados por razones de interés general en la ley, o con el consentimiento del titular de datos, u ordenados por mandato judicial. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. Los datos personales relativos a los antecedentes penales o faltas administrativas solo pueden ser tratados por las autoridades públicas competentes, en la esfera de sus competencias (arts. 3 y 8); c) datos personales relativos a la salud: que son aquellos manejados en hospitales, clínicas, centros y puestos de salud, públicos y privados, y los profesionales vinculados a las ciencias de la salud: solo pueden ser los relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, respetando el secreto profesional (art. 8); d) datos personales comerciales: son datos sensibles de las empresas las bases de datos de clientes, proveedores y recursos humanos, para fines de publicidad y cualquier otros datos que se consideren información comercial o empresarial reservada fundamentalmente para el libre ejercicio de sus actividades económicas (art. 8); e) datos personales de usuarios o compradores: aunque esta categoría no consta descrita en el artículo 8, aparece en el artículo 9 y se refiere al tratamiento que solo debe tener como finalidad facilitar la mejora, ampliación, venta, facturación, gestión, prestación de servicios y adquisición de bienes (art. 9). Además, determina que debe entenderse por ficheros de datos, a los archivos, registros, bases o bancos de datos, públicos y privados, que contienen de manera organizada los datos personales, automatizados o no (art. 3).[1340]

c) Sujeto activo

El artículo 26 de la Constitución nicaragüense reformada en 2014 señala que *toda persona* será sujeto activo del derecho a la protección de datos personales. Dicho eso, es necesario aclarar que respecto a esta forma de redacción existen dos posturas: la primera que señala que al omitir una determinación específica se consideraría que en dicha frase en encuentran incluidas las personas jurídicas; mientras que, para la segunda, otros consideran que al no existir mención expresa se entiende que solo serían titulares las

[1339] Ley No. 787, Ley de Protección de Datos Personales de Nicaragua, 29 de marzo de 2012 - vLex Global.
[1340] Ibíd.

personas naturales.[1341] Ahora bien, esta disyuntiva se resuelve en el ámbito legal, ya que tanto el artículo 1 como el 3 de la Ley 787-2012, Ley de Protección de Datos, señala que su objeto de protección son los titulares, esto es la persona natural o jurídica a la que conciernen los datos personales. Por cuanto el ámbito de aplicación son ficheros públicos y privados, se incluyen estos sujetos activos, pero no hay constancia de que el Estado pueda ser titular de este derecho.

En el artículo 17 literal d) de la Ley 787-2012, Ley de Protección de Datos, se declara el caso especial de los datos que corresponden a personas fallecidas; en este caso serán titulares del derecho los sucesores universales, que deberán probar su condición de herederos.[1342]

d) Sujeto pasivo

Conforme se analizó en líneas anteriores, en las reformas a la Constitución de 1995 constaban como únicos responsables las autoridades estatales. Posteriormente, en las reformas al artículo 26 de la Constitución Política de la República de Nicaragua efectuadas en 2014, se reconoció como responsable tanto a las entidades de naturaleza pública, como a las privadas que registran datos de carácter personal.

El artículo 3, literales l) y k), de la Ley 787-2012, Ley de Protección de Datos Personales, admite como sujetos pasivos al tercero y al responsable de ficheros. El primero sería toda persona, pública o privada que realice a su arbitrio el tratamiento de datos personales, ya sea en ficheros de datos propios o mediante conexión con los mismos; mientras que el responsable de ficheros de datos es toda persona natural o jurídica, pública o privada, que conforme la ley decide sobre la finalidad y contenido del tratamiento de los datos personales. Estableciéndose así la diferencia entre estos dos sujetos pasivos acerca de su responsabilidad respecto a la decisión sobre el tratamiento de los datos o la finalidad y contenido del mismo. En consecuencia, debe señalarse que la normativa nicaragüense no recoge la figura del tercero responsable que realiza por cuenta de otros el tratamiento.

e) Objeto o bien jurídico

a. Derecho de información

El artículo 26 numeral 3 de la Constitución señala que toda persona tiene derecho a conocer de toda información que sobre ella se haya registrado en las entidades de naturaleza privada y pública, así como el derecho de saber por qué y con qué finalidad se tiene esa información. Es decir, el derecho de información no se limita al conocimiento de la información registrada, sino que incluye información respecto de las razones que motivan la recogida y las finalidades de uso de los datos.

b. Autodeterminación informativa

En el artículo 1 de la Ley 787-2012 se señala que su objeto es el resguardo de la información personal como garantía de los derechos fundamentales a la privacidad

[1341] Universidad de Alcalá, "Diccionario de Derechos Humanos - Ver 1.0", 2011, accedido 17 de mayo de 2017, http://diccionario.pradpi.org/inicio/index.php/terminos_pub/view/109.
[1342] Ley 787, Ley de Protección de Datos Personales de Nicaragua, 29 de marzo de 2012 - vLex Global.

personal y familiar y al derecho a la autodeterminación informativa. Ahora bien, el artículo 3, define varios términos propios de la citada ley, y respecto de la autodeterminación informativa dice que: "Es el derecho que tiene toda persona a saber quién, cuándo, con qué fines y en qué circunstancias toman contacto con sus datos personales"[1343].

De ese texto, se colige que existe una confusión pues esta conceptualización estaría limitada al acceso como una de las facultades subjetivas de los titulares, cuando es parte del contenido esencial de este derecho la posibilidad de decidir de forma general sobre cualquier aspecto relativo a sus datos personales. Ahora bien, a lo largo de la ley se describen varias acciones o derechos que pueden ser ejercidos, las que en suma, permiten disponer sobre la recogida, uso, tratamiento, cesión, modificación, eliminación, entre otros. De tal forma, que la autodeterminación se vería materializada aunque la definición no es la más aproximada. Es más, el artículo 5 de la citada ley, determina que para la obtención de datos personales se deben usar medios lícitos que garanticen el derecho de toda persona a la autodeterminación informativa.

La Constitución nicaragüense de 1995 ya establecía en el artículo 26, el derecho de las personas a conocer respecto de sus datos personales y de las finalidades de su recogida y tratamiento, pero no menciona expresamente la facultad de los titulares de decidir sobre estos, que en esta parte sigue vigente. Entre tanto, el considerando quinto de la Ley de Reforma y Adiciones a la Ley 49, "Ley de Amparo", Ley 831 aprobada el 30 de enero del 2013, que incluye por primera vez en Nicaragua como garantía legal al *habeas data* señala que: "este sirve como mecanismo jurisdiccional de protección de los derechos a la autodeterminación informativa y complementa los mecanismos de control de la Constitución que establece la cita Ley".

Finalmente, el artículo 190 de la Carta Magna reformada en 2014, al referirse al *habeas data* determina que este recurso sirve como mecanismo jurisdiccional de protección de los derechos a la autodeterminación informativa, con lo cual el tema quedaría zanjado desde la perspectiva que esta acción prevé los derechos necesarios para ejercer efectivamente el derecho a la autodeterminación informativa.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

El artículo 4 de la Ley 787-2012 determina que será necesaria la autorización de la ley para la creación de ficheros de datos personales en los que no exista consentimiento del titular. Para la licitud del fichero, será necesario que su finalidad esté debidamente determinada.

El artículo 8 de la Ley 787-2012 señala que solo pueden ser obtenidos y tratados por razones de interés general en la ley, o con el consentimiento del titular de datos, u ordenados por mandato judicial. Adicionalmente, solo podrá tratarse con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. Los datos personales relativos a los antecedentes penales o faltas administrativas solo pueden ser tratados por las autoridades públicas competentes, en la esfera de sus competencias.

[1343] Ibíd.

d. Principios

i. Deber de información

El otro lado de la medalla del derecho a la información es el deber que tienen los responsables de los ficheros de informar a los titulares de los datos que tienen registrados, los motivos de la recogida, los tratamientos a los que han sido sometidos los datos y las finalidades de sus usos, tal como señala el artículo 7 de la Ley 787-2012-2012. Pero, además, dicha norma determina otras obligaciones como por ejemplo: el carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, las consecuencias de proporcionar los datos personales, de la negativa a hacerlo o de la inexactitud de los mismos; la garantía de ejercer por parte del titular el derecho de acceso, rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales, entre otros.

ii. Pertinencia

El mismo artículo 19 de la Ley citada, cuando desarrolla el derecho de cancelación señala su procedencia cuando los datos han dejado de ser necesarios o pertinentes para la finalidad que dio lugar a su tratamiento. De esta forma se efectiviza el principio de pertinencia en Nicaragua.

iii. Finalidad

El artículo 26 numeral 3 de la Constitución declara que toda persona tiene derecho de saber por qué y con qué finalidad se ha recogido información personal. Pero, además, es obligación del responsable del fichero informar previamente a los titulares de forma expresa y clara la finalidad para la que serán utilizados y quiénes pueden ser sus destinatarios o clase de destinatarios, conforme consta en el artículo 7 literal a) de la Ley 787-2012-2012. Finalmente, los datos personales solo podrán ser tratados cuando sean adecuados, proporcionales y necesarios en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan solicitado, texto que corresponde al artículo 9 de la citada ley. En general, la finalidad como principio se visibiliza en la recogida de la información, en el tratamiento de los datos, en su cesión y en su vigencia temporal en un fichero, tal como aparece en la normativa nicaragüense.

iv. Calidad

Este principio, aunque no se menciona en la Ley de Protección de Datos, aparece como consecuencia del derecho de solicitar rectificaciones y actualizaciones, toda vez que los responsables deben cuidar la calidad de datos para evitar la interposición de estos pedidos. A pesar de aquello, aparece como causal para que una persona pueda presentar la denuncia propia de la acción de protección de datos, de tal forma que procede si se han lesionado alguno de los principios que rigen la calidad del tratamiento de datos personales, en el ámbito público y privado, conforme el artículo 48 de la Ley de Protección de Datos Personales.

v. Seguridad

Los artículos 9 y 11 de la Ley de Protección de Datos determinan que el responsable del fichero deberá adoptar las medidas de índole técnicas y organizativas necesarias para

garantizar la integridad, confidencialidad y seguridad de los datos y evitar su acceso, uso, alteración, pérdida, revelación, transferencia, tratamiento, consulta, revelación o divulgación no autorizada, y que permitan detectar desviaciones, intencionales o no, de información privada, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Al mismo tiempo, existe una alusión expresa a datos personales difundidos que pudieran afectar la seguridad personal y del Estado, esto es cuando los datos se refieren a miembros de la Policía Nacional o del Ejército de Nicaragua.

El artículo 3 del Reglamento de la Ley 787-2012, Ley de Protección de Datos Personales, Decreto 36-2012, aprobado el 17 de octubre de 2012, al referirse a las definiciones sobre medidas de seguridad establece tres clases: las medidas de seguridad físicas, las medidas de seguridad organizativas y las medidas de seguridad técnicas.

Respecto a las *medidas de seguridad físicas*, señala que estas previenen el acceso no autorizado, el daño o interferencia a las instalaciones físicas, las áreas críticas de la organización, el equipo e información, los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones; los equipos que contienen o almacenan datos personales, todo ello con la finalidad no solo de mantenimiento que asegure la disponibilidad, funcionalidad e integridad, sino a fin de garantizar la eliminación de datos de forma segura.

Acerca de las *medidas de seguridad organizativas*, están dirigidas a establecer mecanismos de gestión, soporte y revisión de la seguridad de la información en el ámbito organizacional, la identificación y clasificación de la información, así como la concientización, formación y capacitación del personal, en materia de protección de datos personales.

Finalmente, sobre las *medidas de seguridad técnicas*, consisten en actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar el control respecto del acceso por parte de usuarios identificados y autorizados y únicamente para las actividades que requieren con motivo de sus funciones. Es indispensable que además se desarrollen acciones de mantenimiento de sistemas seguros.[1344]

vi. Consentimiento

El artículo 3 de la Ley de Protección de Datos señala en los *conceptos* aplicables a la presente ley, el de consentimiento del titular, que es "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular de los datos consiente el tratamiento de sus datos personales"[1345].

Es el reglamento de la Ley 787-2012, Ley de Protección de Datos Personales, en sus artículos 4 al 11 que se establece todo el régimen que permite garantizar un adecuado sistema que garantice el consentimiento. Desarrolla las *características del*

[1344] Nicaragua, "Reglamento de la Ley No. 787, Ley de Protección de Datos Personales", 2012, accedido 14 de mayo de 2017, http://legislacion.asamblea.gob.ni/normaweb.nsf/b92aaea87dac762406257265005d21f7/7bf684022fc4a2b406257ab70059d10f?OpenDocument.

[1345] Ley No. 787, Ley de Protección de Datos Personales de Nicaragua, de 29 de marzo de 2012 - vLex Global".

consentimiento, conforme constan en los artículos 4 y 6 de la ley, señalando como elemento adicional que el consentimiento informado debe ser antes del tratamiento al que serán sometidos sus datos personales.

Que el consentimiento sea inequívoco permite que su manifestación sea expresa o tácita; y conforme el artículo 5 podrá ser tácito, a menos que exista alguna limitación legal. Y deberá ser expreso cuando lo exija una ley o reglamento; se trate de datos financieros o patrimoniales; se trate de datos sensibles; por acuerdo entre titular y el responsable, conforme señala el artículo 7 del referido reglamento. Este consentimiento puede ser escrito o verbal (art. 9), anotándose que conforme señala el artículo 11, la carga de la prueba siempre correrá a cargo del responsable del fichero. Se considerará que el consentimiento expreso se otorgó por escrito cuando el titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por ley. Tratándose del entorno digital, podrán utilizarse firma electrónica o cualquier mecanismo o procedimiento que al efecto se establezca y permita identificar al titular y recabar su consentimiento, conforme reza el artículo 10 del reglamento.[1346]

El consentimiento solo es posible obtenerlo del titular de los datos, o en su defecto de su representante legal o apoderado, salvo excepción legal que debe ser razonable. En caso de controversia, esta razonabilidad deberá ser considerada por la Dirección de Protección de Datos Personales, tanto para ficheros de datos de titularidad pública como privada. El consentimiento deberá ser otorgado por escrito o por otro medio idóneo, físico o electrónico, según el artículo 6 de la citada Ley de Protección de Datos Personales.

El reglamento a la ley determina en el artículo 12 que en cualquier momento el titular de datos podrá revocar su consentimiento y que el responsable del fichero de datos deberá establecer mecanismos sencillos y gratuitos que permitan esta revocatoria. Dicho consentimiento podrá ser revocado sin efecto retroactivo, conforme señala el artículo 6 de la citada Ley de Protección de Datos Personales.

Se podrán prescindir del consentimiento como piedra angular para el ejercicio de la autodeterminación informativa cuando: a. Exista orden motivada, dictada por la autoridad judicial competente; b. Los datos personales se sometan a un procedimiento previo de disociación; c. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; y d. Los datos se obtengan de fuentes de acceso público irrestricto y se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, y fecha de nacimiento, tal como consta en el artículo 6 antes citado.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

a. Derecho de acceso

El artículo 9 de la Ley 787-2012 establece que el derecho de acceso se ejercerá mediante comunicación por escrito dirigida al responsable del fichero. El artículo 17

[1346] Nicaragua, *Reglamento de la Ley 787, Ley de Protección de Datos Personales*.

literal a) del mismo cuerpo legal señala que el titular de los datos personales tiene derecho a solicitar y obtener información de sus datos personales tratados en los ficheros de datos públicos y privados. Por su parte, el reglamento a la ley en el artículo 25 determina que además tendrá derecho a solicitar información relativa a las condiciones y generalidades del tratamiento.

La ley señala que el informe, expuesto en atención a la solicitud del titular de los datos personales, deberá contener la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y las transferencias o cesiones que se realizaron. Por su parte, el reglamento en el artículo 26 determina que se dará por cumplido el derecho de acceso cuando el responsable del fichero de datos ponga en formatos legibles o comprensibles para el titular, a disposición de él, los datos personales en sus oficinas debiendo el remitente conservar la constancia de envío y recepción correspondiente.

El artículo 27 del reglamento determina la gratuidad del ejercicio del Derecho de Acceso a Datos cuando solicite información a la Diprodap relativa a la existencia de ficheros de datos personales, sus finalidades y la identidad de sus responsables, de manera gratuita; y cuando solicite información al responsable del fichero de datos relativa a sus datos personales y al tratamiento dado a los mismos, de manera gratuita una vez al año; se pagará un cargo que cubra el costo de procesamiento, las veces que lo desee.

Finalmente, la Ley 831, Ley de Reforma y Adiciones a la Ley 49, Ley de Amparo, en su artículo 84 bis establece que toda persona puede utilizar dicho recurso para: 1. Acceder a información personal que se encuentre en poder de cualquier entidad pública y privada de la que generen. El mismo artículo 84 sexies señala que, los responsables de los ficheros de datos no pueden alegar confidencialidad de la información que se les requiera, salvo en el caso de que se afecten fuentes de información periodística. Cuando la confidencialidad se alegue en los casos de excepción previstos en la ley, la Sala de lo Constitucional de la Corte Suprema de Justicia puede tomar conocimiento personal y directo de los datos, asegurando el mantenimiento de su confidencialidad.

b. Derecho de rectificación

El artículo 84 bis, numeral 2, de la Ley de Amparo de 2013 establece que: el recurso de *habeas data* faculta a exigir la oposición, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación y actualización de datos personales sensibles independientemente que sean físicos o electrónicos almacenados en ficheros de datos, o registro de entidades públicas o instituciones privadas que brinden servicio o acceso a terceros, cuando se presuma la falsedad, inexactitud, desactualización, omisión total o parcial o la ilicitud de la información de que se trate.

El artículo 7 de la Ley 787-2012 señala: “h. Los datos inexactos, incompletos, o que estén en desacuerdo con la realidad de los que le corresponden a la persona, serán rectificados, modificados, suprimidos, completados, incluidos, actualizados o cancelados según corresponda...”. Por su parte, el artículo 9 señala que los derechos de modificación, inclusión, complementación, rectificación se ejercerán mediante comunicación por escrito. El artículo 17 de la ley en cuestión señala que serán derechos del titular de los datos rectificar, modificar, suprimir, complementar, incluir, actualizar o cancelar sus datos personales. Estas dos normas casi idénticas se complementan y

establecen a la rectificación como derecho base, que se manifiesta en cualquiera de sus formas asimilables. Tan así es que, nuevamente, en el artículo, 19 literal a), consta como derecho el de modificación de los datos que tiene toda persona para solicitar la rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales de los que sea titular, que estén incluidos en un fichero de datos.

El artículo 28 del reglamento determina que la rectificación, de conformidad con lo dispuesto por el artículo 19 de la ley, podrá ser solicitada en todo momento al responsable del fichero de datos que rectifique sus datos personales que resulten ser inexactos o incompletos.

Acerca del procedimiento, en el artículo 19, literal b), de la Ley 787-2012 consta la obligación del responsable del fichero de rectificar, modificar, suprimir, complementar, incluir, actualizar o cancelar los datos personales del titular, dentro de los cinco días hábiles de recibida la solicitud del titular de los mismos, informándole por escrito o por cualquier otro medio que se le equipare según las circunstancias, de manera completa, clara y sencilla el tratamiento realizado. En el literal d) consta, en cambio, la obligación del cesionario de solicitar al responsable de la información que se haya cedido, de actuar también dentro de los cinco días hábiles.

Finalmente, el artículo 48 dice: "La acción de protección de datos personales, procede: [...] c. En los casos en que se presuma la falsedad, inexactitud, desactualización, omisión, total o parcial, o ilicitud de la información de que se trata, para exigir su rectificación, actualización, modificación, inclusión, supresión o cancelación".

El reglamento a la ley determina en el artículo 29 que serán requisitos para el ejercicio del Derecho de Rectificación indicar a qué datos personales se refiere, la corrección que haya de realizarse, así como la documentación que sustente la procedencia de lo solicitado.

El artículo 20 de la ley establece que no procederá la solicitud de modificación cuando exista una resolución judicial que lo determine.

Finalmente, el artículo 21 de la ley señala que la modificación de los datos es gratuita.

c. Derecho de oposición

El artículo 9 de la Ley 787-2012 señala que el derecho de oposición se ejercerá mediante comunicación por escrito.

La ley no determina un contenido específico del derecho de oposición, pero si lo hace el reglamento que lo contempla en la sección V, "Derecho de Oposición", en el artículo 34, que expresamente señala:

> Derecho de Oposición. Para efectos de lo establecido en el artículo 9, párrafo segundo de la Ley, el titular de los datos tiene derecho a que no se lleve a cabo el tratamiento de sus datos personales o se cese en el mismo, cuando no hubiere prestado su consentimiento para su recopilación por haber sido tomados de fuentes de acceso público. Aun cuando hubiere prestado su consentimiento, el titular de los datos tiene derecho a oponerse al tratamiento de sus datos, si acredita la existencia de motivos

> fundados y legítimos relativos a una concreta situación personal que justifiquen el ejercicio de este derecho. En caso que la oposición resulte justificada el responsable del fichero de datos deberá proceder al cese del tratamiento que ha dado lugar a la oposición. No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea requerido por ley.[1347]

Dicho contenido, además de amplio, es significativo respecto de su adecuada delimitación respecto del derecho de cancelación.

d. Derecho de actualización

Este derecho aparece como causal para que una persona pueda presentar la denuncia propia de la acción de protección de datos; de tal forma que procede si se han lesionado alguno de los principios que rigen la calidad del tratamiento de datos personales, en el ámbito público y privado, conforme el artículo 48 de la Ley de Protección de Datos Personales.

e. Derecho de cancelación

El artículo 9 de la Ley 787-2012 señala que el derecho de supresión o cancelación de los datos tratados se ejercerán mediante comunicación por escrito.

El artículo 19 incluye en el derecho de modificación de los datos el de cancelación de datos. Determina que los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad que dio lugar a su tratamiento. La cancelación de los datos no procede por razones de interés social, de seguridad nacional, de salud pública o por afectarse derechos de terceros, en los términos que lo disponga la ley.

Por su parte, el Reglamento de la Ley 787-2012 señala en la sección IV, "Derecho de Cancelación", en el artículo 30 el contenido del derecho de cancelación, pues implica el cese en el tratamiento por parte del responsable del fichero de datos, a partir de un bloqueo de los mismos y su posterior supresión.

El artículo 31 del mismo reglamento señala respecto al ejercicio del derecho de cancelación que el titular de los datos podrá solicitar en todo momento la cancelación de los datos personales cuando hayan dejado de ser necesarios o pertinentes para la finalidad que dio lugar a su tratamiento o cuando considere que los mismos no están siendo tratados conforme a dicha ley y el presente reglamento. La cancelación procederá respecto de la totalidad de los datos personales del titular, contenidos en una base de datos, o solo parte de ellos, según lo haya solicitado.

Asimismo, el artículo 3 de la Ley 787-2012 y los artículos 32 y 33 del reglamento determinan como paso previo a la cancelación el denominado bloqueo,[1348] con el cual se

[1347] Ibíd.

[1348] "Art. 3. Definiciones.- Para la presente ley se entiende por [...] Bloqueo: Es la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en el fichero de datos en el que se

establece un lapso en el que no se pueden tratar y tiene por finalidad establecer posibles responsabilidades por el tratamiento realizado, atender las medidas de seguridad adecuadas para el bloqueo, impedir el tratamiento o posible acceso. El período de bloqueo será de cinco años o hasta el plazo de prescripción legal o contractual correspondiente, así como cuando estos hayan dejado de ser adecuados, proporcionales y necesarios para el ámbito y las finalidades que fueron solicitados, y transcurrido este se procederá a la cancelación de los datos personales en el fichero de datos en el que se encuentran (art. 19, lit. f) de la Ley de Protección de Datos Personales.

f. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

No existe referencia a este derecho en la normativa constitucional, legal o reglamentaria de Nicaragua.

g. Derecho de consulta al registro general de protección de datos personales

El artículo 16 de la Ley 787-2012 señala el derecho a solicitar información a la Dirección de Protección de Datos Personales, relativa a la existencia de ficheros de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita. Esto da cuenta de la obligación que tienen los responsables de ficheros de datos de inscribir en el registro de ficheros de datos de la Dirección de Protección de Datos Personales, conforme consta en el artículo 22 de la citada ley.

El artículo 23 señala que, tanto los ficheros de datos públicos, como los privados solo pueden crearse, modificarse o extinguirse mediante disposiciones establecidas en la presente ley.

h. Derecho a indemnización por daños causados

El artículo 84 duodecies de la Ley de Amparo, reformada en 2013, señala que la Sala de lo Constitucional de la Corte Suprema de Justicia dictará sentencia en la que declarará con lugar el Recurso de *Habeas Data*, ordenará restituir al recurrente en el pleno goce del derecho constitucional vulnerado, la eliminación o supresión inmediata de la información o el dato impugnando; además otorgará al recurrente el derecho a demandar el pago de daños y perjuicios ocasionados, los cuales se liquidarán mediante un proceso de ejecución de sentencia. La sentencia de la Sala de lo Constitucional no impide la utilización de la jurisdicción ordinaria civil y penal para ejercer los derechos mediante las acciones correspondientes.

i. Derecho a confidencialidad

El artículo 84 bis, numeral 3, de la Ley de Amparo de 2013 establece que el recurso de *habeas data* permite exigir la oposición, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación y actualización de cualquier publicidad de datos personales sensibles que lesionen los derechos constitucionales.

---

encuentran". Ley No. 787, Ley de Protección de Datos Personales de Nicaragua, de 29 de marzo de 2012 - vLex Global.

Por su parte, el artículo 84 nonies de la Ley de Amparo, reformada en 2013, señala que si la Sala de lo Constitucional de la Corte Suprema de Justicia determina que se produjo lesión a los derechos del titular de los datos, dictará las medidas que estime pertinentes para el cumplimiento del fallo y velará para que no se divulgue información cuyo titular pueda resultar afectado por el conocimiento que terceros puedan tener de ella, e incluso podrá imponer al recurrente el deber de guardar secreto en relación con lo que conozca, en razón de que el recurso interpuesto fue declarado con lugar.

Por su parte, el artículo 8 de la Ley 787-2012 señala que todos los datos personales solo podrán ser revelados por consentimiento del titular de los datos, por ley expresa de interés social o por mandato judicial.[1349] Por su parte, el artículo 9 de la Ley de Protección de Datos determina que ninguna persona que solicite la prestación o adquisición de bienes y servicios está obligada a brindar a las instituciones públicas y privadas mayor información o datos personales que aquellos que sean adecuados, proporcionales y necesarios para la prestación de los mismos. El artículo 12, respecto de la confidencialidad en el tratamiento de los datos, señala que el responsable del fichero de datos y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el responsable del fichero de datos. Únicamente, podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad nacional, defensa nacional, seguridad pública o la salud pública.

Finalmente, el artículo 17, literal a), de la Ley determina que no se podrá obligar a proporcionar datos personales de carácter sensible, salvo las excepciones establecidas en la presente ley.

j. Derecho al olvido digital

La primera normativa latinoamericana que reconoce el derecho al olvido digital es la nicaragüense. En el artículo 10 de la Ley 787-2012 expresamente señala que el titular de los datos tiene derecho a solicitar a las redes sociales, navegadores y servidores que se supriman y cancelen los datos personales que se encuentren en sus ficheros. En los casos de ficheros de datos de instituciones públicas y privadas, que ofrecen bienes y servicios y que por razones contractuales recopilan datos personales, una vez terminada la relación contractual, el titular de los mismos puede solicitar que se suprima y cancele toda la información personal que se registró mientras era usuario de un servicio o comprador de un bien.

k. Spam

El artículo 26 de la Ley 787-2012, sobre el envío de publicidad no deseada, señala que deberá ofrecerse la posibilidad al destinatario titular de datos personales de expresar su negativa a seguir recibiendo envíos publicitarios y promocionales de bienes y servicios o, en su caso, revocar su consentimiento de una forma clara y gratuita. Además, establece un acto de debida diligencia, exigiendo a las empresas o instituciones que se dedican a actividades de marketing, envíos publicitarios y promocionales electrónicos a que mediante un contrato se establezca que los datos personales han sido obtenidos con

[1349] Ibíd.

el consentimiento inequívoco e informado de los titulares, o que estos han sido obtenidos de fuentes de acceso público.

g) Procedimiento

Los reclamos que se realizan de conformidad con la Ley 787-2012 se dirigen, en primer lugar, al responsable del fichero según señalan los artículos 17 y 19. En segundo lugar, el informe mediante el cual se entregan los datos o se niega motivadamente, se debe proporcionar dentro de los diez días hábiles siguientes a la recepción de la solicitud; vencido el plazo sin que se haya rendido el informe, el interesado puede promover la acción de protección de datos personales prevista en esta ley.

En el artículo 18 de la ley establece que la respuesta a la solicitud de información debe ser clara y sencilla, accesible al conocimiento de la población y al titular de los datos personales; ser amplia y pertenecer al titular, aun cuando lo solicitado solo comprenda un aspecto de los datos personales; puede suministrarse por escrito o por medios electrónicos, telefónicos, de imagen, o por cualquier otro que determine el interesado, a opción del titular, y de acuerdo con la capacidad técnica del responsable de fichero de datos.

Si la solicitud que tuviere fuese negativa, el artículo 13 del reglamento a la ley delimita que el titular de datos podrá presentar ante la Diprodap la denuncia correspondiente. El artículo 35 del mismo reglamento determina que será esta entidad la que realizará la investigación e instrucción del expediente por posibles infracciones. Iniciará la investigación e instrucción del expediente de conformidad al procedimiento administrativo establecido en los artículos del 36 al 52 del reglamento. Constan descritos en el capítulo VII, "De las acciones de protección de datos personales", desde el artículo 47 al 52 el procedimiento pertinente que deberá llevarse a cabo en vía administrativa para la interposición de la acción de protección de datos personales, que deberá dirigirse ante la Dirección de Protección de Datos Personales, órgano encargado de conocer y resolverla.

h) Habeas data

a. Legitimado activo

La Constitución de Nicaragua, reformada en 2014, señala en el artículo 190 que el recurso de *habeas data* procede a favor de toda persona. Por su parte, el artículo 84 ter de la Ley 831, Ley de Reforma y Adiciones a la Ley 49, Ley de Amparo, aprobada el 30 de enero del 2013, establece que el recurso de *habeas data* podrá ser interpuesto por las siguientes personas: a. Persona natural afectada; b. Tutores y sucesores o apoderados de las personas naturales afectadas; c. Personas jurídicas afectadas por intermedio de representantes legales o apoderados designados para tales efectos.

b. Legitimados pasivos u obligados

La citada Ley de Amparo reformada incluye en el artículo 84 quater la expresa referencia a que el recurso de *habeas data* se dirige contra los responsables y cualquier otra persona que hubiere hecho uso indebido de ficheros de datos públicos o privados, o ambos. Se anota que por cuanto se usa el término genérico *cualquier otra persona* que

hubiere hecho uso indebido de ficheros de datos públicos o privados, o ambos, podría entenderse que se incluyen como sujetos pasivos al encargado de tratamiento, al tercero y al destinatario. Anotándose que las categorías tercero y responsable existen en la Ley de Protección de Datos personales.

c. Derechos tutelados por el habeas data

El artículo 5 de la Ley de Amparo reformada expresamente señala:

> Art. 5 bis. El Recurso de Habeas Data se crea como garantía de tutela de datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos, de naturaleza pública o privada, cuya publicidad constituya una invasión a la privacidad personal y tenga relevancia con *el tratamiento de datos sensibles de las personas en su ámbito íntimo y familiar.* El Recurso de *Habeas Data* procede a favor de toda persona para saber quién, cuándo, con qué fines y en qué circunstancias se toma contacto con sus datos personales y su publicidad indebida.[1350] (énfasis añadido)

Completando la norma, el artículo 84 de la Ley de Amparo establece: "Art. 84 bis. El Recurso de *Habeas Data* procede en defensa de los derechos constitucionales reconocidos en el artículo 26 numerales 1, 3 y 4 de la Constitución Política de la República de Nicaragua", es decir, los derechos a la vida privada y familiar, a la honra y reputación y a la autodeterminación informativa. Asimismo, el artículo 190 de la Constitución, cuando menciona *habeas data*, expresamente señala que el ámbito de protección incluye la autodeterminación informativa, cuando determina que también procede a favor de toda persona para saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales.

d. Procedencia del habeas data

El artículo 45 de la Constitución de Nicaragua, reformada en el 2014, dispone que "las personas cuyos derechos constitucionales hayan sido violados o estén en peligro de serlo, pueden interponer el recurso de exhibición personal, de amparo, o de hábeas data, según el caso y de acuerdo con la Ley de Justicia Constitucional"[1351].

El artículo 84 bis de la Ley de Amparo, reformada en 2013, señala que el recurso de *habeas data* procede para: a) acceder a información personal, b) exigir la oposición, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación y actualización cuando se presuma la falsedad, inexactitud, desactualización, omisión total o parcial o la ilicitud de la información de que se trate; c) exigir la oposición, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación y actualización de cualquier publicidad de datos personales sensibles que lesionen los derechos constitucionales.

e. Procedimiento del habeas data

[1350] Asamblea Nacional de Nicaragua, "Ley No. 831, Ley de Reforma y Adiciones a la Ley No. 49, Ley de Amparo".
[1351] "Constitución Política de la República de Nicaragua actualizada con las reformas introducidas por la Ley 854 de 2014, de 29 de enero de 2014 - vLex Global".

Ley 831, Ley de Reforma y Adiciones a la Ley 49, Ley de Amparo, aprobada el 30 de enero del 2013, determina que para interponer el recurso de *habeas data* se requiere que la persona, legitimada procesalmente para ello, previamente haya agotado la vía administrativa contemplada en la Ley 787-2012, Ley de Protección de Datos Personales, publicada en La Gaceta, Diario Oficial 61, del 29 de marzo del 2012 y su Reglamento, Decreto 36-2012, publicado en La Gaceta, Diario Oficial 200, del 19 de octubre del 2012. El recurso se interpondrá dentro de los treinta días posteriores a la notificación de la autoridad administrativa competente en materia de protección de datos personales; se considera también agotada la vía administrativa si dentro del plazo de los treinta días la autoridad administrativa no emite su resolución correspondiente.

El artículo 84 quinquies de la citada ley dispone que sea la Sala de lo Constitucional de la Corte Suprema de Justicia el órgano encargado para conocer y resolver el recurso de *habeas data*. En el artículo 84 septies se determina los requisitos formales del mencionado recurso. Y desde el artículo 84 decies hasta el artículo 84 duodecies consta el procedimiento a seguirse en la Sala de lo Constitucional de la Corte Suprema de Justicia de Nicaragua.

Finalmente, el artículo 84 undecies señala que se puede solicitar una medida precautelatoria con la finalidad de suspender los actos que están produciendo vulneración de derechos cuando el dato se esté transmitiendo y se impugne su confidencialidad; cuando se trate de la inclusión de datos personales sensibles; cuando la impugnación se motive en la inexactitud, falsedad o desactualización de la información y cuando la transmisión de la información o su almacenamiento pueda causar en el futuro, daños irreparables o los cause ilegítimamente.

i) Institucionalidad de protección

Según la Ley de Protección de Datos Personales, la entidad encargada de velar por el cumplimiento y efectiva vigencia del derecho a la protección de datos personales es la Dirección de Protección de Datos Personales, conforme consta en el artículo 28, cuyas funciones constan descritas en el artículo 29, incluyendo la obligación de habilitar el registro de ficheros de datos.

j) Régimen sancionador

En el capítulo VI, relativo a las infracciones y sanciones, específicamente en el artículo 44 de la Ley de Protección de Datos Personales, consta que existen tres niveles de responsabilidad: la administrativa, la civil y la penal. Respecto de la administrativa, se encuentran descritos los tipos de infracción que van desde las leves hasta las graves en el artículo 45. Así como, en el artículo 46 se determinan las sanciones administrativas de los responsables o usuarios de los ficheros de datos.

Según el artículo 30 de la Ley de Protección de Datos de 2012, además de establecer institucionalidad de protección, se ha diseñado un sistema de control basado en figuras de vigilancia denominadas “inspectores”, conforme se desprende del artículo 31. Los procedimientos de inspección, responsabilidades, atribuciones del inspector y demás elementos del sistema de control están descritos en los artículos 32 hasta el 43 de la citada norma.

El artículo 56 del reglamento a la Ley de Protección de Datos Personales establece que será Diprodap la que iniciará el procedimiento de imposición de sanciones cuando determine presuntas infracciones a la ley y a las regulaciones que de ella se deriven, susceptibles de ser sancionadas según al artículo 46 de la misma. Finalizado el procedimiento respectivo, se emitirá la resolución correspondiente. Sobre el procedimiento consta descrito desde el artículo 57 hasta el 60 del reglamento.

k) Transferencia internacional de datos

El artículo 13 de la Ley de Protección de Datos Personales señala que se podrán ceder y transferir datos personales con el consentimiento previo del titular de los datos, a quien se le deberá informar sobre la finalidad de la cesión e identificar al cesionario. El consentimiento para la cesión es revocable, mediante notificación por escrito o por cualquier otra vía que se le equipare. El artículo 14 señala las prohibiciones y excepciones de cesión y transferencia de datos cuando otros países u organismos internacionales no proporcionen niveles de seguridad y protección adecuados. La prohibición no regirá en los supuestos de colaboración judicial internacional, intercambio de datos personales en materia de salud, cuando sea necesaria para una investigación epidemiológica, transferencias bancarias o bursátiles, conforme la legislación de la materia; cuando la transferencia se hubiere acordado en el marco de tratados internacionales ratificados por el Estado de Nicaragua; y cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia, en los delitos de prevención, investigación y persecución del crimen organizado.

Finalmente, existe una normativa sectorial que regula únicamente los datos personales que están en manos del Estado, la cual rigió durante mucho tiempo pero ha sido superada por la actual normativa previamente analizada. Esta es la Ley 621, aprobada el 16 de mayo del 2007, publicada en La Gaceta 118, del 22 de junio del 2007, denominada Ley de Acceso a la Información Pública.

2.8 Venezuela (1999)

La Constitución de Venezuela de 1999 señala en el título III, De los derechos humanos y garantías, y de los deberes, capítulo I, de las disposiciones generales que consagra el derecho a la intimidad, a la vida privada, al honor, a la propia imagen a la confidencialidad, a la reputación y como su garantía al *habeas data*.

Respecto de la intimidad y el honor, el artículo 60 los reconoce en su forma primigenia, pero además expresamente señala, tal como lo hace la normativa constitucional española, la protección al honor y a la intimidad de los abusos de la informática de tal forma que determina que será la ley la que la limite. Desde esta visión, se protege el dato personal pero solo aquel considerado íntimo. Esta posición se ha superado en general en la mayoría de legislaciones porque es precisamente la naturaleza del dato por sí mismo, y no su caracterización de íntimo o sensible, la que determina la necesidad de protección.

> Artículo 60. Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la

> informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.[1352]

Asimismo, el artículo 28 de la Constitución consagra al *habeas data* en el texto siguiente:

> Artículo 28. Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley.[1353]

Debido a que el título III, De los derechos humanos y garantías, y de los deberes, no establece un capítulo pertinente a garantías constitucionales; se entienden que estos son reconocidos en la medida en la que se describen los derechos. Por lo tanto, de la estructura y de la redacción del texto constitucional se colige que Venezuela no se consagra el derecho a la protección de datos personales, sino la garantía del *habeas data* que busca proteger los derechos descritos en el artículo 60: honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. Y en tal virtud, permite el acceso a los datos personales, al conocimiento de las finalidades de su captura; así como a su actualización, rectificación o destrucción, pero en garantía de los citados derechos, por eso es que la norma requiere que los datos sean erróneos o que afecten ilegítimamente sus derechos para su procedencia.

Sustenta dicha interpretación, el contenido del artículo 281 que señala expresamente:

> Artículo 281. Son atribuciones del Defensor o Defensora del Pueblo: [...] 3. Interponer las acciones de inconstitucionalidad, amparo, habeas corpus, *habeas data* y las demás acciones o recursos necesarios para ejercer las atribuciones señaladas en los ordinales anteriores, cuando fuere procedente de conformidad con la ley.[1354]

Es decir, le otorga al defensor del pueblo la atribución de interponer la acción de *hábeas data*, sin que exista en el resto del texto constitucional otra norma a la cual atribuírsele esta remisión.

Oscar Pucinelli, respecto de la forma en la que la Constitución de Venezuela aborda el tema, señala que:

> La norma contiene cuanto menos, tres aciertos: el primero, el de incluir la versión de hábeas data impropio,[1355] que había sido incorporado por primera vez en la Constitución peruana; el segundo, el de extender la garantía de confidencialidad de la fuente de la

[1352] Venezuela, Asamblea Nacional Constituyente, *Constitución de la República Bolivariana de Venezuela*, *Political Database of the Americas*, 1999, accedido 12 de julio de 2017, http://pdba.georgetown.edu/Constitutions/Venezuela/vigente.html.
[1353] Ibíd.
[1354] Ibíd.
[1355] Se refiere al artículo 143 de la Constitución venezolana por la cual se faculta el acceso a información pública contenida en ficheros estatales.

> información a otras profesiones distintas del periodismo, y el tercero, que constituye una novedad distintiva, el reconocimiento de la facultad del defensor del pueblo de interponer la acción de hábeas data, lo que en definitiva puede considerarse la partida de nacimiento normativa del hábeas data colectivo.[1356]

De la cita del autor se desprende que el *habeas data impropio* se refiere al derecho de acceso a información pública contenida en ficheros estatales, descrito en artículo 143 de la Constitución venezolana con el texto siguiente:

> Artículo 143. Los ciudadanos y ciudadanas tienen derecho a ser informados e informadas oportuna y verazmente por la Administración Pública, sobre el estado de las actuaciones en que estén directamente interesados e interesadas, y a conocer las resoluciones definitivas que se adopten sobre el particular. Asimismo, tienen acceso a los archivos y registros administrativos, sin perjuicio de los límites aceptables dentro de una sociedad democrática en materias relativas a seguridad interior y exterior, a investigación criminal y a la intimidad de la vida privada, de conformidad con la ley que regule la materia de clasificación de documentos de contenido confidencial o secreto. No se permitirá censura alguna a los funcionarios públicos o funcionarias públicas que informen sobre asuntos bajo su responsabilidad.[1357]

Se aclara que, respecto de este derecho fundamental hasta la actualidad no existe normativa legal específica que desarrolle los criterios generales del mismo, sino que su regulación se encuentra dispersa en distinta regulación sectorial.[1358]

En el año 2009, la Sala Constitucional del Tribunal Supremo de Justicia dictó la resolución 1511/2009,[1359] de 9 de noviembre en el caso Mercedes Josefina Ramírez en Acción de *Habeas Data*:[1360] "en la que una vez resuelta la admisión de una solicitud de *habeas data*, estableció de forma general y abstracta un procedimiento más breve que permitiera –en su criterio– una pronta decisión judicial en este tipo de procesos constitucionales, modificando el que hubiera establecido en la sentencia 2551/2003, de 24 de septiembre"[1361]. Dicha jurisprudencia sigue vigente pues no ha existido norma

[1356] PUCCINELLI, *Tipos y subtipos*, 11.

[1357] Venezuela, Asamblea Nacional Constituyente, *Constitución de la República Bolivariana de Venezuela*, *Political Database of the Americas*, 1999.

[1358] Mirador Democrático, "Normas venezolanas sobre acceso a la información en poder del Sector Público al 2002 (Selección no exhaustiva)", *Organización de Estados Americanos*, 2002, accedido 19 de julio de 2017, http://www.oas.org/es/sla/ddi/docs/VE2%20Normas-Venezolanas-sobre-Acceso-a-la-Informacion-e.pdf.

[1359] Sala constitucional del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela, "Nueva jurisprudencia vinculante sobre el procedimiento de *Habeas Data* | Constitucional | "Sentencia No. 1511/2009 en el caso: Mercedes Josefina Ramírez en Acción de *Habeas Data*", 2009, accedido 19 de julio de 2017, https://jurisprudencia.tuabogado.com/constitucional/nueva-jurisprudencia-vinculante-sobre-el-procedimiento-de-habeas-data.

[1360] Sala Constitucional del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela, "Sentencia No. 1511/2009 en el caso: Mercedes Josefina Ramírez en Acción de *Habeas Data*", *Tribunal Supremo de Justicia de la República Bolivariana de Venezuela*, 2009, accedido 12 de julio de 2017, http://www.tsj.gov.ve/decisiones/scon/Noviembre/1511-91109-2009-09-0369.html.

[1361] J. A. BERRÍOS ORTIGOZA, "La reconfiguración del proceso constitucional de *habeas data*. Estudio sobre (a decisión 1511/2009, de 9 de noviembre de la Sala Constitucional del Tribunal Supremo de Justicia - vLex Global", *Fronesis Revista de Filosofía Jurídica, Social y Política*, vol. 16, 3 (2009), accedido 12 de julio de 2017, https://app-vlex-com.bibliotecavirtual.udla.edu.ec/?r=true#WW/search/*/Sentencia+No.++1511%2F2009+VENEZUELA/vid/211625409.

posterior que la modifique conforme aparece de las sentencias 569,[1362] 297[1363] y 336[1364] que la siguen aplicando.

No existe norma general para proteger los datos personales en Venezuela. Únicamente, varias de carácter sectorial que se las analizará a continuación:

a. *Ley Infogobierno*, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Número 40.274, del 17 de octubre de 2013,[1365] aplicable exclusivamente al sector gubernamental. Cuya finalidad, entre otras, es la de garantizar la interoperabilidad del Poder Público con el Poder Popular, y en consecuencia asegurar un flujo adecuado, proporcionado y seguro de datos personales. Sobre las normas y el funcionamiento de este subsistema se describirá en la descripción del contenido esencial, ya que aunque no son normas de aplicación general son las únicas que pueden ser invocadas en determinados temas.

b. *Ley de Registro de Antecedentes Penales*, publicada en la Gaceta Oficial 31.791, el 3 de agosto de 1979,[1366] que establece la obligación de registrar los datos personales de las personas condenadas por sentencia definitiva firme, y que establece como sanción penal la pena de tres (3) a quince (15) meses de prisión al funcionario que revele, comunique o publique los datos contenidos en el Registro de Antecedentes Penales (art. 13).

c. *Ley sobre Protección a la Privacidad de las Comunicaciones*, publicada en la Gaceta Oficial 34.863, el 16 de diciembre de 1991,[1367] por el cual se protege la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones (art. 1) para evitar que persona alguna de forma arbitraria, clandestina o fraudulentamente grabe o se imponga de una comunicación, interrumpa o la impida, so pena de recibir sanción penal de prisión de tres (3) a cinco (5) años. La misma ley establece en casos debidamente sustentados responsabilidad penal de gravedad para quienes revelen, en todo o en parte, mediante cualquier medio de información, el contenido de las comunicaciones personales (art. 2). Con la debida justificación y autorización judicial previa (arts. 7 y 8), se establecen

[1362] Sala Constitucional del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela, "Sentencia No. 569", *vLex Global*, 2010, accedido 12 de julio de 2017, https://app-vlex-com.bibliotecavirtual.udla.edu.ec/?r=true#WW/search/content_type:2/%221511%2F2009%22/WW/vid/283243847.

[1363] Sala Constitucional del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela, "Sentencia No. 297", *vLex Global*, 2010, accedido 12 de julio de 2017, https://app-vlex-com.bibliotecavirtual.udla.edu.ec/?r=true#WW/search/*/Sentencia+No.++1511%2F2009+VENEZUELA/WW/vid/283254939.

[1364] Sala Constitucional del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela, "Sentencia No. 336", 2010, accedido 12 de julio de 2017, https://app-vlex-com.bibliotecavirtual.udla.edu.ec/?r=true#WW/search/*/%221511%2F2009%22/p3/WW/vid/283231931.

[1365] Asamblea Nacional República Bolivariana de Venezuela, "Ley De Infogobierno, Gaceta No. 40274", 2013, accedido 11 de julio de 2017, http://www.asambleanacional.gob.ve/leyes/_ley-de-infogobierno.

[1366] Asamblea Nacional de la República Bolivariana de Venezuela, "Ley de Registro de Antecedentes Penales, Gaceta Oficial 31.791", *Red Hemisférica de Intercambio de información para la asistencia mutua en materia penal y extradición*, 1979, accedido 12 de julio de 2017, https://www.oas.org/juridico/mla/sp/ven/sp_ven-mla-law-antec.html.

[1367] Asamblea Nacional de la República Bolivariana de Venezuela, "Ley sobre Protección a la Privacidad de las Comunicaciones, Gaceta Oficial No. 34.863", *Conatel Venezuela*, 1991, accedido 12 de julio de 2017, http://www.conatel.gob.ve/ley-sobre-proteccion-a-la-privacidad-de-las-comunicaciones-2/.

casos excepcionales de interceptación, interrupción, grabación con fines investigativos de hechos punibles relacionados con la seguridad e independencia del Estado, patrimonio público, sustancias estupefacientes y psicotrópicas, secuestro y extorsión (art. 6).

d. *Ley Orgánica para la Protección de Niños, Niñas y Adolescentes*, publicada en la Gaceta Oficial 5.859, del 10 de diciembre de 2007.[1368]

   Respecto al derecho al honor, reputación, propia imagen, vida privada e intimidad familiar de niños, niñas y adolescentes, se los protege de las injerencias arbitrarias o ilegales por parte de terceros. De tal forma que se prohíbe exponer o divulgar, a través de cualquier medio, imágenes, datos o informaciones de niños, niñas y adolescentes contra su voluntad o la de su padre, madre, representantes o responsables, o que pudieren lesionar su honor o reputación, o que permitan identificar, directa o indirectamente, a los niños, niñas y adolescentes que hayan sido sujetos activos o pasivos de hechos punibles, salvo autorización judicial fundada en razones de seguridad u orden público (art. 65).

   Asimismo, entre las atribuciones de la Defensoría del Pueblo se encuentra la de ejercer la acción de *habeas data* para la aplicación de medidas de protección ante los consejos de efectos particulares en beneficio de niños, niñas y adolescentes (art. 170-A, lit. h).

   Respecto de la confidencialidad del proceso de adopción y el derecho del adoptado a partir de los doce años de solicitar acceso a la información de su expediente de adopción (art. 429).

   Finalmente, en virtud de la confidencialidad, se prohíbe la publicación de datos de la investigación o del juicio que, directa o indirectamente, posibiliten identificar al adolescente. Se dejan a salvo las informaciones estadísticas y el traslado de pruebas (art. 545).

e. *Ley Especial contra los Delitos Informáticos*, publicada en la Gaceta Oficial 37.313, de octubre de 2001.[1369] Dicha norma establece en las definiciones, de manera general, el concepto de data o datos al que se hará referencia en la parte pertinente (art. 2).

   Asimismo, el capítulo III, titulado "De los delitos contra la privacidad de las personas y de las comunicaciones", establece los siguientes tipos penales en garantía de este bien jurídico protegido:

[1368] Asamblea Nacional de la República Bolivariana de Venezuela, "Ley Orgánica para la Protección de Niños, Niñas y Adolescentes, Gaceta Oficial 5.859", *Ministerio Público de la República Bolivariana de Venezuela*, 2007, accedido 12 de julio de 2017, http://www.ministeriopublico.gob.ve/c/document_library/get_file?uuid=f59b4caf-ed38-495b-b7ba-14a4556e0a7c&groupId=10136.

[1369] Asamblea Nacional de la República Bolivariana de Venezuela, "Ley Especial Contra los Delitos Informáticos, Gaceta Oficial 37.313.", *Conatel Venezuela*, 2001, accedido 12 de julio de 2017, http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-Especial-contra-los-Delitos-Inform%C3%A1ticos.pdf.

a) *Violación de la privacidad de la data o información de carácter personal*. Este tipo penal establece que "Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero" (art. 20).

b) *Violación de la privacidad de las comunicaciones.* Por el cual "Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias" (art. 21).

c) *Revelación indebida de data o información de carácter personal.* Establece que "Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad" (art. 22).

f. Decreto 9.051, mediante el cual se dicta el *Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*, Gaceta Oficial 39.945, del 15 de junio de 2012.

   El artículo 43 señala expresamente que "entre órganos y entes del Estado están obligados a compartir los datos de autoría, y sólo podrán excusarse de compartir los datos, información y documentos que manejan cuando la ley expresamente así lo limite, a fin de garantizar la protección al honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de los ciudadanos y ciudadanas". [1370]

Como las normas previamente citadas son de aplicación limitada a un ámbito o sector, para identificar el contenido esencial del derecho a la protección de datos personales en Venezuela se acudirá a la norma constitucional y a la jurisprudencia generalmente obligatoria a la que se hizo referencia en líneas anteriores. La norma sectorial, si bien puede ser orientativa por su carácter parcial, no puede ser tomada como elemento

[1370] Presidencia de la República Bolivariana de Venezuela, "Decreto N° 9.051, Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado. Gaceta Oficial 39.945", *Conatel Venezuela*, 2012, accedido 15 de julio de 2017, http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-sobre-Acceso-e-Intercambio-Electr%C3%B3nico-de-Datos.pdf.

sustancial de la conformación del derecho, por lo que solo será invocada si es que no existe otra norma y recordando siempre su condición acotada.

a) Ámbito: Registros o ficheros públicos y privados

Del análisis únicamente exegético del artículo 28 de la Constitución, se desprende que el *habeas data* puede ejercitarse respecto de datos que consten en registros oficiales o privados, con las excepciones que establezca la ley.

b) Naturaleza del dato

La norma constitucional señala los términos datos e información como sinónimos. Además, es necesario recalcar que se realiza la precisión de que los datos están vinculados a una persona cuando en la norma consta que esta se referirá a datos *sobre sí misma o sobre sus bienes*.

Se utiliza los términos registros oficiales o privados y no bases o bancos de datos, con lo que no se asocia el término únicamente a procesos informáticos o automatizados, sino que pareciera referirse a registros de datos físicos. Se utiliza también el término documento, determinando que este podrá ser de cualquier naturaleza con tal que contenga información cuyo conocimiento sea de interés para comunidades o grupos de personas. Bajo esta redacción se entiende que uno de los soportes válidos será el documento mismo que podrá ser material o electrónico.

Como no existe normativa específica para el concepto de dato podemos acudir a la Ley especial contra los delitos informáticos de 2001, que en el artículo 2, del título I, disposiciones generales, al referirse a las definiciones aplicables a esta ley se entiende por "Data (datos): hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar un significado".

c) Sujeto activo

En el artículo 28 de la Constitución se señala como sujeto activo a *toda persona*, de tal manera que tanto personas naturales como jurídicas se configuran como sujetos activos de la garantía del *habeas data*. Pero además, la misma norma realiza la precisión de que las comunidades o grupos de personas pueden ser sujetos activos respecto de aquella *información cuyo conocimiento le es de interés*.

Como sujeto activo coadyuvante, la propia Constitución determina que se le atribuye al Defensor del Pueblo la facultad de interponer la acción de *habeas data* (art. 281 de la Constitución). Asimismo, entre las facultades de la Defensoría del Pueblo está la de presentar acción de *habeas data* para la aplicación de medidas de protección ante los consejos de efectos particulares en beneficios de niños, niños y adolescentes (art. 170-A, lit. h) *Ley Orgánica para la Protección de Niños, Niñas y Adolescentes*, publicada en la Gaceta Oficial 5.859, del 10 de diciembre de 2007.[1371]).

[1371] Asamblea Nacional de la República Bolivariana de Venezuela, "Ley Orgánica para la Protección de Niños, Niñas y Adolescentes, Gaceta Oficial 5.859".

d) Sujeto pasivo

Conforme señala la norma constitucional, artículo 28, serán sujetos pasivos aquellos que tienen a cargo los registros oficiales o privados. No pueden ser sujetos pasivos aquellos que tengan información en virtud del secreto de las fuentes periodísticas o del ejercicio de aquellas profesiones determinadas en la ley, como por ejemplo de aquellas relacionadas con la salud.

e) Objeto o bien jurídico

a. Derecho de información

El artículo 28 de la Constitución señala que toda persona tiene derecho a conocer el uso que se haga de sus datos personales y la finalidad de la recogida de estos. De esta manera, queda configurado el derecho de información como parte del contenido esencial de la garantía constitucional del *habeas data*.

b. Autodeterminación informativa

La ausencia de mención alguna, en la Constitución y en normativa vigente, a la autodeterminación informativa, es decir sobre este poder de control o decisión sobre los datos personales, sería la evidencia de que el derecho a la protección de datos personales no ha sido reconocido en Venezuela, sino que aún se ata la protección del dato personal a otros derechos fundamentales. En consecuencia, es indispensable el reconocimiento del derecho en el ámbito legal o constitucional, y en tal sentido dotarle de contenido independiente y autónomo sobre todo de la intimidad y de la privacidad, además una ley de carácter general que pueda aplicarse a todos los ámbitos y sectores. La ausencia de la autodeterminación informativa se manifiesta en el artículo 28 de la Constitución que señala como única forma de justificar el ejercicio de los derechos de rectificación, actualización o destrucción en lo equivocado de los datos o la afectación ilegítima de sus derechos, y no la simple voluntad de su titular.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

La norma constitucional señala en el artículo 28 que es necesaria una ley expresa para limitar los derechos del titular de acceder, conocer el uso que se haga de sus datos personales o de sus bienes, su finalidad. En la misma norma citada se deja a salvo y no es posible acceder, ni aun con mandato legal, al secreto de las fuentes de información periodística y de otras profesiones que determine la ley; estas últimas generalmente asociadas a servicios de salud.

Otro ejemplo de necesidad de ley expresa que faculte a recopilar o acceder datos personales es el artículo 78 de la Ley de Infogobierno, por la cual solo con solicitud previa de la persona legitimada, el Poder Público y el Poder Popular pueden recopilar y utilizar datos de niños, niñas y adolescentes para las finalidades para las cuales se solicitaron que serán siempre relacionadas a sus derechos y garantías consagradas en la Constitución y la ley.

d. Principios

i. Deber de información

El artículo 28 de la Constitución, referente básico en este análisis, no hace mención alguna a los principios del derecho a la protección de datos personales. Cuando habla de información, lo hace desde la perspectiva del derecho de información no desde la obligación del responsable del fichero de entregar esta so pena de recibir algún tipo de asignación de responsabilidad o sanción.

El artículo 78 de la Ley de Infogobierno señala que para el caso de registro de datos de niños, niñas y adolescentes, el receptor de los datos debe priorizar e indicar los derechos que le asisten y la normativa aplicable para llevar a cabo el trámite solicitado en beneficio del niño, niña o adolescente; es decir, un deber de información general y específico en garantía de este grupo vulnerable.

En los numerales 22, 23 y 24 del artículo 41 de la Ley de Infogobierno de 2013, para incentivar el intercambio electrónico de datos, información y documentos; el análisis de problemáticas comunes, la realización de proyectos conjuntos en materia de tecnologías de información; y en consecuencia, constituir un estándar de interoperabilidad determina como obligaciones de la Comisión Nacional de las Tecnologías de Información: a) establecer mecanismos de coordinación y colaboración entre el Poder Público y el Poder Popular, b) garantizar el cumplimiento de las políticas, lineamientos, normas y procedimientos; c) resolver los conflictos que surjan en relación al acceso e intercambio electrónico de datos, de información y documentos o al uso inadecuado de estos. Debe aclararse que esta norma no se aplica para datos personales sino que, en concordancia con el citado artículo 43 del Decreto 9.051, mediante el cual se dicta el *Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado*,[1372] se refiere a datos de autoría; es decir, aquellos que provienen del Estado, como resultado del cumplimiento de los procesos administrativos que realiza con ocasión al ejercicio de sus atribuciones o como resultado de la tramitación de las diligencias, actuaciones o gestiones que realizan las personas ante ellos (art. 2, Decreto 9.051). Y en consecuencia, los órganos estatales cuando lo señale la ley, podrán excusarse de compartir datos, información y documentos en garantía al honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas (art. 43, Decreto 9.051*)*.

Este intercambio de información en el ámbito estatal puede entenderse como un deber de información que permita una adecuada comunicación para la garantía del funcionamiento de la administración pública y el ejercicio de los derechos de participación, pero no como parte del contenido esencial del derecho a la protección de datos personales.

ii. Pertinencia

No existe referencia a este principio en la normativa general. Ahora bien, la Ley de Infogobierno señala en el artículo 22 del capítulo II, Principios y bases del uso de las tecnologías de información, el principio de proporcionalidad que determina que en las actuaciones que realicen el Poder Público y el Poder Popular mediante las tecnologías

[1372] Presidencia de la República Bolivariana de Venezuela, "Decreto 9.051, Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado. Gaceta Oficial 39.945".

de información, solo se exigirán a las personas los datos que sean estrictamente necesarios para tramitar los asuntos que hayan solicitado, a los fines de garantizar el cumplimiento de los principios y derechos establecidos en la Constitución de la República y la ley. Esta norma recoge una aproximación al principio de pertinencia aunque su ámbito de aplicación es limitado al sector público.

iii. Calidad

No existe referencia a este principio en la normativa general ni específica.

iv. Finalidad

El artículo 28 de la Constitución menciona el derecho de las personas a conocer la finalidad del registro oficial o privado de sus datos personales. En este sentido no se ha previsto como principio que permita controlar la actuación de los responsables del fichero, sino como parte del derecho de información, es decir, del derecho a conocer para qué se utilizarán sus datos.

v. Seguridad

En la Ley de Infogobierno de 2013 existe la mención a la necesidad de salvaguardar la seguridad de los datos que estén bajo la responsabilidad de entes estatales. Este deber se le asigna a la Superintendencia de Servicios de Certificación Electrónica, a la cual en el artículo 54 se le considera el órgano competente en materia de seguridad informática y responsable del desarrollo, implementación, ejecución y seguimiento al Sistema Nacional de Seguridad Informática, de implementar entre el Poder Público y el Poder Popular las iniciativas de seguridad informática, dirigidas a la privacidad, protección de datos y de infraestructuras críticas, así como intervenir y dar respuesta ante los riesgos y amenazas que atenten contra la información que manejen (art. 55), a fin de resguardar la autenticidad, integridad, inviolabilidad y confiabilidad de los datos, información y documentos electrónicos (art. 54).

Entre los subsistemas que conforman el Sistema Nacional de Protección y Seguridad Informática constan los siguientes: 1. Subsistema de Criptografía Nacional, 2. Subsistema Nacional de Gestión de Incidentes Telemáticos, 3. Subsistema Nacional de Informática Forense, 4. Subsistema Nacional de Protección de Datos (art. 57); este último se entiende incluye datos, información, documentos y datos personales.

vi. Consentimiento

No existe mención sobre el consentimiento en la norma constitucional. Únicamente la Ley de Infogobierno al referirse a datos de niños, niñas y adolescentes señala en el artículo 79, la obligación de contar con el consentimiento previo de su representante legal, salvo cuando el menor de edad sea emancipado, en la investigación de hechos punibles, por una orden judicial, o cuando así lo determine la ley. Se determina, además, que el consentimiento expreso que se haya dado sobre la información siempre puede ser revocado.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

a. Derecho de acceso

El artículo 28 de la Constitución señala el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley. Este es el principal contenido de la garantía del *habeas data*, pues por su intermedio se conoce y revisa si los datos son correctos o si generan o no daños a sus derechos fundamentales para proceder a solicitar su rectificación, actualización o destrucción.

Esta norma tiene una innovación y es la de reconocer el derecho de acceso a comunidades o grupos de interés con la condición básica de que contengan información cuyo conocimiento sea de su interés.

b. Derecho de rectificación

La Constitución venezolana en el artículo 28 señala que toda persona podrá solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos datos personales que fuesen erróneos o afectasen ilegítimamente los derechos de sus titulares. Estos requisitos, como se analizó previamente, significan un sistema de protección de los datos personales atado a la intimidad.

c. Derecho de oposición

No existe referencia a este principio en la normativa general ni específica.

d. Derecho de cancelación

El artículo 28 de la Constitución señala que toda persona podrá solicitar ante el tribunal competente la destrucción de aquellos datos personales que fuesen erróneos o afectasen ilegítimamente los derechos de sus titulares. Manifestación clara de la ausencia del derecho a la autodeterminación informativa pues no permite la eliminación de dato por simple voluntad de su titular.

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

No existe referencia a este principio en la normativa general ni específica.

f. Derecho de consulta al registro general de protección de datos personales

No existe referencia a este principio en la normativa general ni específica.

g. Derecho a indemnización por daños causados

No existe referencia a este principio en la normativa general ni específica.

h. Derecho a la confidencialidad

Sobre el principio de confidencialidad, la norma constitucional menciona en la parte final del artículo 28 que no se podrá acceder, ni conocer el uso, ni la finalidad de la recogida y registro, ni la actualización, la rectificación o la destrucción de la información que se llegue a conocer en relación con la profesión que se profesa o secreto profesional, así como el secreto de las fuentes periodísticas.

Ahora bien, en el artículo 74 de la Ley de Infogobierno se determina que toda la información que conste en los archivos y registros en el Poder Público y en el Poder Popular es de carácter público, excepto aquella información sobre el honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas, la seguridad y defensa de la nación, de conformidad con lo establecido en la Constitución de la República, la ley que regule la materia sobre protección de datos personales y demás leyes que rigen la materia. De esta manera, se establece como regla la confidencialidad de los datos personales; lamentablemente no se reconoce a la protección de datos personales como el derecho del cual emane este sistema de salvaguarda, sino que expresamente se sigue atando al derecho a la intimidad, a la privacidad e incluso se menciona al honor, la reputación y la propia imagen.

i. Derecho al olvido digital

No existe referencia a este principio en la normativa general ni específica.

j. Spam

No existe referencia a este principio en la normativa general ni específica.

g) Procedimiento

Por no existir normativa legal no se ha desarrollado un procedimiento de carácter legal.

h) Habeas data

A continuación se describirá el procedimiento constitucional desarrollado jurisprudencialmente mediante la sentencia de aplicación obligatoria, Resolución 1511/2009,[1373] de 9 de noviembre, en el caso "Mercedes Josefina Ramírez en Acción de Habeas Data":

a. Sujeto activo

Como se analizó en líneas precedentes, el artículo 28 de la Constitución señala como sujeto activo a *toda persona como legitimado activo para interponer* la garantía del *habeas data*; de tal forma que en esta generalización se incluye, tanto a la persona natural como a la jurídica. Y como se vio, la misma norma menciona que las

[1373] Sala constitucional del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela, "Nueva jurisprudencia vinculante sobre el procedimiento de *Habeas Data* | Constitucional | "Sentencia No. 1511/2009 en el caso Mercedes Josefina Ramírez en Acción de *Habeas Data*".

comunidades o grupos de personas pueden ser sujetos activos respecto de aquella *información cuyo conocimiento es de su interés.*

Será sujeto activo coadyuvante, el Defensor del Pueblo de conformidad con el artículo 281 de la Constitución que le establece la facultad de interponer acción de *habeas data*. Por eso, entre las facultades de la Defensoría del Pueblo consta la de presentar la acción de *habeas data* en beneficios de niños, niñas y adolescentes (art. 170-A, lit. h) *Ley Orgánica para la Protección de Niños, Niñas y Adolescentes*, publicada en la Gaceta Oficial 5.859, 10 de diciembre de 2007).[1374]

b. Sujetos pasivos u obligados

Según lo ya analizado en esta investigación, el artículo 28 de la Constitución dispone que los legitimados pasivos de la garantía de *habeas data* serán aquellos que tienen a su cargo los registros oficiales o privados. Y por disposición expresa de carácter constitucional, no pueden ser sujetos pasivos aquellos que tengan información en virtud del secreto de las fuentes periodísticas o del ejercicio de aquellas profesiones determinadas en la ley.

c. Derechos tutelados por el habeas data

La norma constitucional, en el artículo 28 no menciona expresamente qué derechos son los tutelados por el *habeas data*, pero al ser una garantía constitucional protege en esencia los derechos descritos en el artículo 60: honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas.

Por eso, la Ley de Infogobierno menciona en el artículo 25 que el uso de las tecnologías de información por el Poder Público y el Poder Popular comprende la protección del honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas; en consecuencia, está sujeto a las limitaciones que establezca la ley sobre la materia.

d. Procedencia del habeas data

Nuevamente, del análisis del artículo 28 de la Constitución solo procede el *habeas data* respecto de la posibilidad de rectificación, actualización o destrucción cuando los datos personales fuesen erróneos o afectasen ilegítimamente los derechos del titular; de tal manera que es necesario, primero, probar estas condiciones para que la acción prospere. Del mismo modo, respecto al derecho de acceso solo será posible el ejercicio de este cuando los datos son de quien solicita la garantía y, siempre y cuando, no exista una ley que lo impida.

e. Procedimiento del habeas data

Se establece un procedimiento para la garantía constitucional de *habeas data* mediante una jurisprudencia de aplicación obligatoria dictada por la Sala Constitucional del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela, la resolución

[1374] Asamblea Nacional de la República Bolivariana de Venezuela, "Ley Orgánica para la Protección de Niños, Niñas y Adolescentes, Gaceta Oficial 5.859".

1511/2009,[1375] de 9 de noviembre, en el caso "Mercedes Josefina Ramírez" que señala tres elementos fundamentales del proceso:

i. El proceso se iniciará por escrito y deberá identificar las pruebas que desea promover y consignar el documento fundamental de su pretensión, que conforme sentencia 1281/2006, caso "Pedro Reinaldo Carbone Martínez"[1376] consiste en cualquier documento que sirva como medio probatorio de la existencia indiscutible de los registros que se quieren rectificar, destruir o actualizar mediante *habeas data*, con lo cual se modifica el criterio anterior que aceptaba acciones de *habeas data* que no contaban con este documento fundamental fallo 2.829, 7 de diciembre de 2004.[1377]

ii. Debidamente notificada la parte demandada y el Fiscal General de la República, se convocará a una audiencia oral y pública a menos que esté prohibida por la ley o afecte la moral y las buenas costumbres y en ella las partes alegarán su defensa. La Sala Constitucional decretará cuáles son las pruebas admisibles y necesarias. En la audiencia y evacuación de pruebas se velará por la igualdad de las partes y el derecho de defensa.

iii. La sentencia se dictará por el tribunal dentro de los cinco días siguientes a la audiencia.

i) Institucionalidad de protección

No existe referencia a este principio en la normativa general ni específica.

j) Régimen sancionador

No existe referencia a este principio en la normativa general. Ahora bien, en la Ley de Infogobierno, únicamente aplicable al ámbito público, consta el artículo 81 que establece infracciones y multas, y por tanto sanciones administrativas, sin perjuicio de la responsabilidad civil cuando emplee para fines distintos a los solicitados, los datos, información o documentos obtenidos mediante un servicio de información.

k) Transferencia internacional de datos

No existe referencia a este principio en la normativa general ni específica.

2.9 Chile (1999)

Conforme consta en el documento titulado Historia de la Constitución Política, artículo 19, núm. 4 de la Biblioteca del Congreso Nacional de Chile, la primera vez que se

[1375] Sala constitucional del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela, "Nueva jurisprudencia vinculante sobre el procedimiento de *Habeas Data* | Constitucional | "Sentencia No. 1511/2009 en el caso Mercedes Josefina Ramírez en Acción de *Habeas Data*".

[1376] J. CUERVO, "Decisión 1281/2006. Tribunal Supremo de Justicia. Sala Constitucional, 26 de junio de 2006. s/ *Habeas Data*. Expediente 05-1964. Magistrada Ponente: Carmen Zuleta de Merchán", *Informática Jurídica*.

[1377] J. CUERVO, "Decisión 2829/2004. Tribunal Supremo de Justicia. Sala Constitucional, 7 diciembre 2004, s/ *Habeas Data*. Expediente 04-0733. Magistrado Ponente: Antonio J. García García", *Informática Jurídica*.

discutió la necesidad de regular la privacidad consta recogida en las Actas Oficiales de la Comisión Ortúzar 1.1. Sesión 85, 7 de noviembre de 1974, en el cual aparece expresamente que:

> [...] los países más adelantados han desarrollado legislaciones sobre el derecho a la privacidad o a la intimidad, que es una distinción más del respeto a la dignidad humana y, por lo mismo, se trata de una materia cuyo establecimiento sería novedoso...[1378]

Es en la sesión 1.9. Sesión 416, 5 de octubre de 1978, en la cual se acordó el texto que ahora consta consagrado en el artículo 19.4 de la Constitución Política de Chile, Decreto Ley 3464, 8 de agosto de 1980, aunque es solo hasta la que determina lo siguiente:

> Artículo 19.- La constitución asegura a todas las personas: [...] 4º. El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.[1379]

Posteriormente, en las reformas incluidas por la Ley 20.050 de 2005 elimina de la norma constitucional el término vida *pública* por cuanto, conforme se señaló en los debates y en el informe de la Comisión Constitucional que expresamente sostuvo: "Se elimina la noción de «protección de vida pública» por no resultar claro sus alcances ni interpretación, por no tener parangón en el derecho constitucional comparado ni en el derecho internacional de los derechos humanos ni por ser una norma que manifieste alguna utilidad…". Informe Comisión de Constitución. Senado, 16 de agosto de 2005. Informe verbal en Sesión 26, Legislatura 353.[1380]

Fuera de lo analizado, la Constitución de la República de Chile de 1980, texto refundido, coordinado y sistematizado, DTO-100 22-SEP-2005,[1381] expresamente señala:

> Artículo 19.- La Constitución asegura a todas las personas: [...] 4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia...

En otras palabras, se protege la vida privada, lo que determina un menor nivel de protección, ya que no se consagran ni el derecho a la protección de datos personales, ni a la autodeterminación informativa; es decir, no reconoce este derecho fundamental propio de la era tecnológica, que es el único que permite una tutela completa del individuo y su dignidad en la sociedad red.

Con ese enfoque limitado se ha dictado una normativa denominada Ley 19.628, 28 de agosto de 1999 de Protección a la Vida Privada, que ha sido modificada mediante las siguientes normas: Ley 19.812, 13 de junio de 2002; Ley 20.463, 25 de octubre de 2010, Ley 20.521, 23 de julio de 2011; Ley 20.575, 17 de febrero de 2012, de

---

[1378] M. S. G. de la Presidencia de la República de Chile, "Historia de la Constitución Política, artículo 19 Nº 4, DTO-100 22-SEP-2005 Ministerio Secretaría general de la Presidencia", *Ley Chile - Biblioteca del Congreso Nacional*, 2005, accedido 18 de noviembre de 2017, https://www.leychile.cl/Navegar?idNorma=242302#privacidad0.

[1379] Ibíd.

[1380] Ibíd.

[1381] Ministerio Secretaría General de la Presidencia, "Constitución de la República de Chile, Texto refundido, coordinado y sistematizado. DTO-100 22-SEP-2005", *Ley Chile - Biblioteca del Congreso Nacional*, 2005, accedido 18 de enero de 2018, https://www.leychile.cl/Navegar?idNorma=242302%20.

modificación de la Ley 19.628,[1382] sin que ninguna de estas modificaciones haya podido perfilar un reconocimiento del derecho a la protección de datos personales en Chile ya que la mayoría de ellas se refieren únicamente a datos crediticios.

En el año 2000 consta el Decreto 779/2000, 11 de noviembre de 2000, por el cual se reglamenta la Ley 19.629, que regula el Registro de Bancos de Datos Personales a Cargo de los Organismos Públicos;[1383] esta norma es de carácter sectorial pues su aplicación se limita al ámbito público.

Otra norma de aplicación general es la Ley 19.223, 7 de junio de 1993, relativa a Delitos Informáticos (arts. 1º-4º) que incluye normativa para proteger la vida privada y la honra.[1384]

De otro lado, respecto de datos públicos existe la norma expresa que regula el tema; esta es la LEY-20285, 20 de agosto de 2008 sobre acceso a la información pública.[1385]

Se debe tomar como elemento de análisis las Recomendaciones del Consejo para la Transparencia, de 14 de septiembre de 2011, sobre datos personales en manos de la Administración del Estado.

En el año 2018 se aprobó el proyecto a la protección de datos personales en un derecho constitucional por parte de la Cámara de Diputados, por lo que ahora resta la comunicación al Ejecutivo del gobierno del presidente Sebastián Piñera para que la norma sea promulgada. Por esta iniciativa se modifica el núm. 4, del artículo 19º del Texto Constitucional, que asegura "el respeto y protección a la vida privada y a la honra de la persona y su familia" en el siguiente sentido: "4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley...".

Finalmente, se encuentran en primer trámite constitucional ante la Cámara de Diputados de Chile un proyecto que fue enviado por la Presidenta Michelle Bachelet a través del Boletín 11144-07, refundido con una moción parlamentaria ubicada en el Boletín 11092-07[1386]. En estas normativas se pretende crear un órgano independiente, especializado y autónomo que pueda velar eficientemente por el derecho a la protección

[1382] M. S. G. de la Presidencia, "LEY-19628 28-AGO-1999 Ministerio Secretaría General de la Presidencia, sobre protección de la vida privada", *Ley Chile - Biblioteca del Congreso Nacional*, 1999, accedido 20 de noviembre de 2017, https://www.leychile.cl/Navegar?idNorma=141599&buscar=SOBRE+PROTECCION+DE+LA+VIDA+PRIVADA.

[1383] Ministerio de Justicia de Chile, "DTO-779 11-NOV-2000 que aprueba Reglamento del Registro de Banco de Datos Personales a Cargo de Organismos Públicos", *Ley Chile - Biblioteca del Congreso Nacional*, 2000, accedido 18 de enero de 2018, https://www.leychile.cl/Navegar?idNorma=177681.

[1384] Ministerio de Justicia de Chile, "LEY-19223 07-JUN-1993 Tipifica Figuras Penales relativas a la informática", *Ley Chile - Biblioteca del Congreso Nacional*, 1993, accedido 18 de enero de 2018, https://www.leychile.cl/Navegar?idNorma=30590.

[1385] Ministerio Secretaría General de la Presidencia, "LEY-20285 20-AGO-2008 sobre acceso a la información pública", *Ley Chile - Biblioteca del Congreso Nacional*, 2008, accedido 18 de enero de 2018, https://www.leychile.cl/Navegar?idNorma=276363.

[1386] Cámara de Diputados de Chile, "Proyectos de Ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales", accedido el 27 de agosto de 2018, https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07

de datos personales. Además, dicho proyecto incluye categorías de datos como los biométricos, establece derechos como el de rectificación, obligaciones a los responsables de tratamiento, infracción y un sistema sancionatorio, cuestiones que no existen en la versión actual de normativa de protección de datos en Chile.

a) Ámbito: Registros o ficheros públicos y privados

La Ley 19628, 29 de agosto de 1999, sobre protección de la vida privada, en el título preliminar, denominado "Disposiciones generales", artículo 1º, señala que el tratamiento de los datos de carácter personal se realizará en registros o bancos de datos regidos, tanto por organismos públicos como por particulares.

b) Naturaleza del dato

La citada Ley 19628 en el artículo 2º determina que para efectos de esta ley se entenderá por: a) datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables; b) datos sensibles, aquellos que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual —en este concepto llama la atención la inclusión de datos relativos a hábitos personales, de tal forma que se consideran por su naturaleza íntima y por lo tanto sensible—; c) dato estadístico, el que en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

El título III, denominado utilización de datos personales relativos a obligaciones de económico, financiero, bancario o comercial ha sido ampliamente desarrollado en dos leyes modificatorias: Ley 19812 y Ley 20575.

Ese título determina que la naturaleza general de los datos personales crediticios es ser datos personales con carácter económico, financiero, bancario o comercial. Cuando este carácter consta en letras de cambio y pagarés protestados, cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa, como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, así como aquellas debidamente sustentadas que determine el Presidente de la República (Ley 20575, art. 7º a), D.O. 17.02.201), entre otras de carácter mercantil, pueden ser entregadas a terceros. Pero no podrán serlo si dicha información está relacionada con créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario o relativas a créditos redactados, renegociados o novados, de conformidad con la Ley 19812, art. 1º, núm. 2, D.O. 13.06.2002; es decir, se reconoce un sistema de protección a créditos de apoyo rural y aquellos en los que hay una voluntad de saneamiento de la obligación mediante cualquiera de los mecanismos jurídicos y económicos implementados para el efecto.

En el mismo sentido, no podrá publicar o comunicar información relacionada con deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas; tampoco podrán comunicarse las deudas contraídas con concesionarios de autopistas por el uso de su infraestructura (Ley 19812, art. 1º, núm. 3, D.O. 13.06.2002) o cuando estas se hayan originado durante el período de

cesantía que afecte al deudor (Ley 20575, art. 7º b), D.O. 17.02.2012); o cuando han transcurridos cinco años desde que la respectiva obligación se hizo exigible o esta ha sido pagada o extinguido por otro modo legal.

Como se ve, la normativa chilena desarrolla ampliamente el régimen de datos crediticios estableciendo una serie de excepciones que están dirigidas a evitar discriminaciones a personas que por condiciones económicas podrán tener condición de deudoras y afectárseles sus derechos al no tomar en cuenta su precariedad.

Otras definiciones descritas en la normativa señalan: a) Dato caduco, el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna; b) Procedimiento de disociación de datos, todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable; c) Registro o banco de datos, el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos; d) Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes; y e) Tratamiento de datos, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma (Ley 19628, art. 2º).

c) Sujeto activo

Conforme el artículo 2º de la Ley 19628, se concibe al titular de los datos como la persona natural a la que se refieren los datos de carácter personal.

d) Sujeto pasivo

La citada norma, artículo 2º de la Ley 19628, describe al responsable del registro o banco de datos como la persona natural o jurídica privada, o el respectivo organismo público, a quienes competen las decisiones relacionadas con el tratamiento de los datos de carácter personal.

Se establece en el literal k) del señalado artículo 2 que serán organismos públicos, las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1º de la Ley 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado.

Finalmente, el artículo 8° de la Ley 19628 determina que si el tratamiento de datos personales se efectúa por mandato, se aplicarán las reglas generales. En otras palabras, el mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos.

e) Objeto o bien jurídico

a. Derecho de información

No existe referencia a este derecho en la normativa general ni específica.

b. Autodeterminación informativa

No existe referencia a este derecho en la normativa general ni específica.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

En el artículo 4º del título I, relativo a la utilización de datos personales, se determina que el tratamiento de datos personales solo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen, o el titular consienta expresamente en ello. Asimismo, cuando no existe consentimiento del titular es necesario mandato legal para el tratamiento de datos sensibles (art. 10º, Ley 19628). La ley establece la salvedad de no necesitar autorización del titular cuando los datos permitan el otorgamiento de beneficios de salud que correspondan a sus titulares (art. 14º), cuando provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios (art. 4º). Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquellos (art. 4º), o cuando los datos personales están en un banco de datos al cual tienen acceso diversos organismos (art. 14º), señalándose además que el titular puede requerir información a cualquiera de ellos.

d. Principios

i. Deber de información

Conforme señala el artículo 3º de la Ley 19628, en toda recolección de datos personales que se realice mediante encuestas, estudios de mercado o sondeos de opinión pública u otros, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información.

El citado artículo 4° de la Ley 19628 determina que la persona que autoriza el tratamiento de sus datos debe ser debidamente informada respecto del propósito del almacenamiento y su posible comunicación al público; en resumen establece una forma básica de deber de información asociada al consentimiento del uso de los datos personales.

Asimismo, el artículo 12 de la citada ley señala el derecho de los titulares a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al

tratamiento de datos personales a entregar información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

ii. *Pertinencia*

No existe referencia a este principio en la normativa general ni específica.

iii. Calidad

Aunque refiriéndose a finalidad de los datos, el artículo 9° de la Ley 19628 determina que los datos personales deben ser exactos, actualizados y responder con veracidad a la situación real de su titular. Todos estos elementos que pueden configurar el contenido del principio de calidad de datos.

iv. Finalidad

El artículo 9° de la Ley 19628 establece que los datos personales deben utilizarse solo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público.

Respecto de datos crediticios, cabe determinar la prohibición de realizar todo tipo de predicciones o evaluaciones de riesgo comercial que no estén basadas únicamente en información objetiva relativa a las morosidades o protestos de las personas naturales o jurídicas de las cuales se informa. La infracción a esta prohibición obligará a la eliminación inmediata de dicha información por parte del responsable de la base de datos y dará lugar a la indemnización de perjuicios que corresponda (Ley 20521, art. UNICO, D.O. 23.07.2011.

v. Seguridad

No existe referencia a este principio en la normativa general ni específica.

vi. Consentimiento

El artículo 4º de la Ley 19628 especifica que la persona titular del dato debe autorizar, por escrito, su tratamiento para los propósitos para los que se solicitó su almacenamiento y su posible comunicación al público. Podrá ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.

vii. *Confidencialidad*

El título final que contiene el artículo 24 de la Ley 19628 agrega los incisos segundo y tercero, al artículo 127º del Código Sanitario que dice:

> Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro

> Décimo. Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

a. Derecho de acceso

Aunque no consta descrito el derecho de acceso, sin embargo, en el artículo 13º de la Ley 19628 se dice que el derecho de las personas a la información no puede ser limitado por medio de ningún acto o convención. En el mismo sentido, el artículo 14º determina que si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos. Finalmente, el artículo 15º señala los límites de este acceso cuando establece que no podrá solicitarse información, cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la nación o el interés nacional.

En el artículo 2º, literal i), consta la descripción de fuente accesible al público, considerándola como aquellos registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

b. Derecho de rectificación

El literal j) del artículo 2º de la Ley 19628 determina que se entiende como modificación de datos, todo cambio en el contenido de los datos almacenados en registros o bancos de datos.

Entre uno de los posibles cambios es aquel que se desprende del derecho de sus titulares a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, a que en caso de acreditarse que los datos personales sean erróneos, inexactos, equívocos o incompletos deban ser modificados, de forma gratuita, conforme el artículo 12º de la citada norma. Además, podrá proporcionarse, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho.

Tal como se señaló anteriormente, el artículo 15 determina que no podrá solicitarse modificación cuando con ello se pudiera afectar el cumplimiento de las funciones fiscalizadoras del organismo público o se afecte la reserva o secreto.

Un caso común de modificación es el descrito en el artículo 19º de la ley en mención determina que al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, este avisará tal hecho, a más tardar dentro de los

siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, con el pago previo de la tarifa si fuere procedente, con cargo al deudor. El deudor podrá optar por requerir directamente la modificación al banco de datos y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito.

c. Derecho de oposición

Aunque no consta descrito el derecho de oposición en sentido estricto, sin embargo, aparecen menciones cuando se describe que el consentimiento puede ser revocado sin efecto retroactivo (art. 4º). Asimismo, el artículo 3° de la ley determina que "El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión".

d. Derecho de cancelación

Conforme señala, tanto el artículo 6º como el artículo 12º de la Ley 19628, sin perjuicio de las excepciones legales, podrá eliminarse (que consiste en la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello [art. 2º]) o bloquearse datos personales (por el cual se suspende de forma temporal cualquier operación de tratamiento de datos almacenados [2º]) cuando su almacenamiento carezca de fundamento legal, estuvieren caducos, cuando si bien fueron proporcionados voluntariamente o se usen para comunicaciones comerciales y ya no se desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

Se añade que si los datos personales cancelados o modificados hubieren sido comunicados previamente (comunicación o transmisión de datos: que permite dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas [art. 2º]), el responsable del banco de datos deberá avisarles a la brevedad posible; y si no fuese posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos.

Se anota que conforme el artículo 6º se bloqueará los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación; en estos casos se procederá a la eliminación, modificación o bloqueo de los datos, sin necesidad de requerimiento del titular.

Finalmente, según el artículo 13º, el derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención.

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

Al tenor de lo señalado, en el artículo 5º de la Ley 19628 se determina que el responsable del banco de datos personales podrá:

> [...] establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes. Frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de: a) La individualización del requirente; b) El motivo y el propósito del requerimiento, y c) El tipo de datos que se transmiten. La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga. El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión. No se aplicará este artículo cuando se trate de datos personales accesibles al público en general. Esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes.

f. Derecho de consulta al registro general de protección de datos personales:

En el artículo 22º se determina que será el Servicio de Registro Civil e Identificación, el que llevará un registro de los bancos de datos personales a cargo de organismos públicos. Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende; todo lo cual será definido en un reglamento. El organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca. Como se colige, la obligación de registro es exclusiva de las autoridades públicas ante un organismo limitado únicamente a registrarla y que no puede realizar ningún tipo de acción de resguardo, prevención o protección con tal registro; menos aún ponerlo como parte de un derecho de consulta vinculante para el titular como para el responsable.

g. Derecho a indemnización por daños causados

El artículo 11º de la Ley 19628 establece que el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños. Esta norma, al determinar un régimen de responsabilidad, establece de manera directa el derecho a la indemnización por los daños que pudieran causarse.

Asimismo, el artículo 23º de la Ley 19628 señala que la persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo con lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

h. Derecho a la confidencialidad

Al tenor del artículo 7º, se determina que las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes

relacionados con el banco de datos; obligación que no cesa por haber terminado sus actividades en ese campo.

i. Derecho al olvido digital

No existe referencia a este derecho en la normativa general ni específica.

j. Spam

La Ley de Protección del Consumidor; Ley 19.496, 7 de febrero de 1997, reformada por la Ley 19955, art. único n.º 20, D.O. 14.07.2004 que señala expresamente lo siguiente:

> Artículo 28 B.- Toda comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la materia o asunto sobre el que versa, la identidad del remitente y contener una dirección válida a la que el destinatario pueda solicitar la suspensión de los envíos, que quedarán desde entonces prohibidos. Los proveedores que dirijan comunicaciones promocionales o publicitarias a los consumidores por medio de correo postal, fax, llamados o servicios de mensajería telefónicos, deberán indicar una forma expedita en que los destinatarios podrán solicitar la suspensión de las mismas. Solicitada ésta, el envío de nuevas comunicaciones quedará prohibido.

La protección del *spam* en Chile se encuentra en una ley distinta a la de datos personales, más bien relacionada con derechos del consumidor.

g) Procedimiento

Por no existir normativa constitucional que reconozca la acción constitucional, en Chile al *habeas data* se lo considera como la acción legal que consta descrita en la Ley 19628 y que se analizará a continuación.

h) Habeas data

a. Sujeto activo

En el artículo 2º de la Ley 19628 se concibe al titular de los datos como la persona natural a la que se refieren los datos de carácter personal.

b. Sujetos pasivos u obligados

El artículo 2º de la Ley 19628 describe al responsable del registro o banco de datos como la persona natural o jurídica privada, o el respectivo organismo público, a quienes competen las decisiones relacionadas con el tratamiento de los datos de carácter personal.

El artículo 8° de la Ley 19628 determina que en el caso de que el tratamiento de datos personales se efectúe por mandato, se aplicarán las reglas generales. Dicho de otro modo, el mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos.

c. Derechos tutelados por el habeas data

El artículo 12º de la Ley 19628 comprende los derechos que se garantizan al titular, entre los que constan el derecho de información al mencionar respecto del derecho de toda persona a exigir la "información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente".

Alude además al derecho de modificación mencionando que "en caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen".

Atiende al derecho de cancelación o bloqueo plasmando que el titular puede exigir respecto de sus datos que "se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos" y añade "cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo".

Y a pesar de que no lo expone de manera explícita añade el derecho de gratuidad exteriorizando que "la información, modificación o eliminación de los datos serán absolutamente gratuitas".

Y concluye con el artículo 15º con la excepción a la efectivización de estos derechos en los casos en los que ello afecte con "el debido cumplimiento de las funciones fiscalizadoras (…) la reserva o secreto (…) la seguridad de la Nación o el interés nacional".

d. Procedencia del habeas data

Conforme el artículo 12º de la Ley 19628, el *habeas data* procede contra toda responsable de un banco que se dedique en forma pública o privada al tratamiento de datos personales, tanto por el requerimiento de información como por la rectificación, modificación, eliminación o bloqueo cuando los datos sean erróneos, inexactos, equívocos o incompletos, carezcan de fundamento legal o cuando estuvieren caducos o cuando no deseen continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

e. Procedimiento del habeas data

Conforme a lo señalado en el artículo 16º, se determina el procedimiento aplicable a cualquier acción presentada en sede judicial que requiera cualquiera de los derechos descritos en el literal precedente.

El procedimiento señala que si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable.

Entonces, según lo señalado en el artículo 16º de la Ley 19628:

> [...] el procedimiento se sujetará a las reglas siguientes: a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso. b) El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte. c) El

> responsable del banco de datos deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada. d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere la letra anterior, sea que se hayan o no presentado descargos. Si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta. e) Todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario. f) La sentencia definitiva será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan. g) Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes. h) El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación. En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente. La sala de la Corte Suprema que conozca la reclamación conforme al inciso anterior, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento establecido en los incisos primero y segundo, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. En las reclamaciones por las causales señaladas en el inciso precedente, el Presidente del Tribunal dispondrá que la audiencia no sea pública. En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales, o de diez a cincuenta unidades tributarias mensuales si se tratare de una infracción a lo dispuesto en el artículo 17. La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el Tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días.

En suma, de la negativa del responsable de la base de datos cabe acción judicial y de esta resolución el recurso de apelación, pero no procede el recurso de casación por disposición expresa.

i) Institucionalidad de protección

La normativa chilena no señala la autoridad que precautele el derecho a la protección de datos personales almacenados por responsables públicos o privados. Como se ha visto en líneas precedentes, la acción de *habeas data* es resuelta en sede judicial. Si bien, la Ley 20.285 determina que será el Consejo de la Transparencia el que vele por el ejercicio de la Ley 19.628, sin embargo, se limita únicamente al derecho de acceso a la información pública.

j) Régimen sancionador

El título V, denominado "De la responsabilidad por las infracciones a esta ley", en el artículo 23º de la Ley 19628 señala que la acción de *habeas data* podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción. En todo caso, las infracciones no contempladas en los artículos 16º y 19º, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez. El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

k) Transferencia internacional de datos

No existe referencia en la normativa general ni específica.

l) Del tratamiento de datos por los organismos públicos

En la Ley 19628 el título IV, relativo al tratamiento de datos por los organismos públicos en los artículo 20º, 21º y 22º hace referencia al régimen que deben cumplir los organismos públicos para tratar datos personales, esto es solo efectuarlas respecto de las materias de su competencia de tal manera que aplicando la ley no necesitará el consentimiento del titular. Respecto de organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena. Se exceptúan los casos en que esa información les sea solicitada por los tribunales de justicia u otros organismos públicos dentro del ámbito de su competencia, los cuales deberán guardar respecto de ella la debida reserva o secreto y, en todo caso, les será aplicable lo dispuesto en los artículos 5º, 7°, 11º y 18º; todo ello al tenor del artículo 21.

2.10 Bolivia (2002)

En la Constitución Política del Estado de 1967, el artículo 7º determinaba que toda persona tiene derechos fundamentales; entre ellos el literal l) señalaba el derecho al nombre, a la intimidad y privacidad personal y familiar, así como a su imagen, honra y reputación *(inciso agregado por la Ley 2410, 8 de agosto 2002).*

Posteriormente, la Constitución de la República de Bolivia de 2009 abroga la Constitución Política del Estado de 1967 y sus reformas posteriores y determina en el artículo 21 el texto siguiente:

> Artículo 21º.- Las bolivianas y los bolivianos tienen los siguientes derechos: [...] 2. A la privacidad, intimidad, honra, honor, propia imagen y dignidad...[1387]

La actual normativa boliviana realiza varias precisiones que favorecen la amplitud del contenido de los varios derechos enlistados en la citada norma. Así, por ejemplo, se

[1387] Asamblea Nacional Constituyente de Bolivia, "Bolivia: Constitución, 2009", 2009, accedido 18 de septiembre de 2017, http://pdba.georgetown.edu/Constitutions/Bolivia/bolivia09.html.

eliminan de la norma las especificidades de una intimidad, privacidad o imagen personal y familiar, permitiendo que estos derechos puedan ser comprendidos incluso en contextos ajenos a esas esferas, con la precisión de que basta que la imagen sea propia. Asimismo, incluye tanto el término honra como honor, de tal manera que se protege tanto la percepción interna como la externa de una persona en sociedad. Finalmente, menciona el fin primigenio de cualquier construcción social, esto es la dignidad humana. Se concluye que la vigente norma constitucional amplía el rango de protección de todos los derechos enlistados, y además lo vuelve preciso y enmarcado en su finalidad: la dignidad humana.

Así también, la Constitución Política del Estado de 1967, *modificada por la Ley 2410, 8 de agosto 2002, que* actualmente se encuentra derogada, determinaba al *habeas data* como acción constitucional con el texto siguiente:

> Artículo 23º.- Acción de *Habeas Data* por el cual: I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de *Habeas Data* ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya. II. Si el tribunal o juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado. III. La decisión que se pronuncie se elevará en revisión, de oficio ante el Tribunal Constitucional, en el plazo de veinticuatro horas, sin que por ello se suspenda la ejecución del fallo. IV. El recurso de *Habeas Data* no procederá para levantar el secreto en materia de prensa. V. El recurso de *Habeas Data* se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el Artículo 19º de esta Constitución (artículo modificado por la Ley 2410, 8 de agosto de 2002).[1388]

Como se señaló previamente, dicha norma fue derogada y en su lugar la vigente Constitución de 2009 determina en el capítulo segundo, relativo a las acciones de defensa, una denominada "Acción de Protección de Privacidad", constante en el artículo 130, que estipula:

> Artículo 130. I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad. II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.

En el siguiente artículo de la Constitución de 2009, esto es el artículo 131, se detalla el procedimiento propio de esta acción de protección de privacidad:

> I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional.

[1388] Asamblea Nacional Constituyente de Bolivia, "Constitución Política de 1967, con reformas de 1994, texto concordado de 1995, y reformas de 2002, 2004 y 2005", 1967, accedido 18 de septiembre de 2017, http://pdba.georgetown.edu/Constitutions/Bolivia/consboliv2005.html.

> II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado.
>
> III. La decisión se elevará, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución.
>
> IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme con lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la ley.

El Tribunal Constitucional, a través de varias sentencias ha dado contenido a la acción de protección de la privacidad asimilándola, aunque no en denominación, pero si en sustancia al *habeas data*. La autora Karina Medinaceli cita varias sentencias de la Corte Constitucional, para delinear la línea jurisprudencial establecida sobre esta temática. La resolución No. 0189/2010-R de fecha 24 de mayo de 2010 establece la relación entre *habeas data* y acción de protección de privacidad al tenor del siguiente texto:

> […] es imperante determinar con claridad el objeto y la causa del presente recurso de hábeas data, actualmente denominado acción de protección de privacidad, razón por la cual, se tiene que en la especie, el objeto de la tutela pedida es la eliminación de datos supuestamente falsos cursantes en los archivos públicos de la INTERPOL y la Dirección Nacional de Identificación, para la protección de los derechos de los recurrentes a la dignidad, a la vida privada, a la honra, al honor, a la reputación y a la personalidad[…]

En sentido similar, la Sentencia Constitucional 0965/2004 de fecha 23 de junio de 2004 y otras sentencias constitucionales, "crean las subreglas en relación al derecho a la autodeterminación informática, reconoce la protección de la persona jurídica, la actualización de los datos, la confidencialidad y los datos sensibles, entre otros"[1389], conforme consta del siguiente texto:

> […] el hábeas data es una garantía constitucional que tiene por objetivo contrarrestar los peligros que conlleva el desarrollo de la informática en lo referido a la distribución o difusión ilimitada de información sobre los datos de la persona; tiene por finalidad principal proteger el derecho a la autodeterminación informática, preservando la información sobre los datos personales ante su utilización incontrolada, indebida e ilegal, impidiendo que terceras personas usen datos falsos, erróneos o reservados que podrían causar graves daños y perjuicios a la persona […] En cuanto a los límites del Hábeas Data, es importante remarcar que, como vía procesal instrumental, protege a la persona en su derecho a la autodeterminación informática, activándose contra el poder informático. De manera que cabe advertir que existe un límite en cuanto a los alcances del hábeas data que se establece en el ejercicio de la libertad o derecho de información y libertad de expresión […]

Respecto del procedimiento de la acción de protección de privacidad, si bien consta en la Constitución que se estará a lo dispuesto para la acción de amparo, el 5 de julio de 2012 se dicta Código Procesal Constitucional[1390] que establece un procedimiento propio.

[1389] K. I. MEDINACELI, *El tratamiento de los datos sanitarios en la historia clínica electrónica: Caso boliviano* (Madrid: Agencia Española de Protección de Datos Personales, 2017), 210.

[1390] Asamblea Legislativa Plurinacional de Bolivia, "Código Procesal Constitucional", *Portal Jurídico Lex Ivox libre*, accedido 5 de julio de 2012, accedido el 27 de agosto de 2019, https://www.lexivox.org/norms/BO-L-N254.html

Sobre el derecho de acceso a la información pública, la Constitución de la República de Bolivia de 2009 determina en el artículo 21:

> Artículo 21. Las bolivianas y los bolivianos tienen los siguientes derechos: [...] 6. A acceder a la información, interpretarla, analizarla y comunicarla libremente, de manera individual o colectiva.[1391]

Lamentablemente, Bolivia no consagra una normativa específica sobre el derecho a la protección de datos o, como se denomina, protección de privacidad. No existe un sistema general de protección, sino normas sectoriales que intentan regular este derecho y que son las que se listan a continuación:

- Ley 1768, Ley de Modificaciones al Código Penal, 10 de marzo de 1997, emitida por el Congreso Nacional del Estado Plurinacional de Bolivia.[1392] Por el cual se incluye en el Código Penal, el capítulo XI, del título XII, del Libro Segundo del Código Penal, con la denominación "Delitos Informáticos", los artículos 363 bis y 363 ter.

  El artículo 363 bis, del Código Penal, determina el tipo penal de manipulación informática, que sanciona la intrusión digital (*hackers*). Por su parte, el artículo 363 ter del Código Penal señala el tipo penal de alteración, acceso y uso indebido de datos informáticos, que sanciona a quien comete una intrusión para hacerse de datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información. Esta norma es la que puede aplicarse en defensa de datos en general y en especial de datos personales.

- Decreto Supremo 28168, 17 de mayo de 2005, por el cual se abroga el Decreto Supremo 27329, 31 de enero de 2004, que garantiza el acceso a la información, como derecho fundamental de toda persona y la transparencia en la gestión del poder.[1393]

- Ley 018, Ley del Órgano Electoral Plurinacional de Bolivia, 16 de junio de 2010, emitido por el Congreso Nacional del Estado Plurinacional de Bolivia.[1394] En el artículo 72 establece, entre las obligaciones del Servicio de Registro Cívico (Sereci), el respeto irrestricto del derecho a la intimidad e identidad de las personas y los demás derechos derivados de su registro, así como la garantía de la privacidad y confidencialidad de los datos registrados de las personas y la

[1391] Asamblea Nacional Constituyente de Bolivia, "Bolivia: Constitución, 2009", cit.
[1392] Asamblea Legislativa Plurinacional de Bolivia, "Ley 1768, Ley de Modificaciones al Código Penal de 10 de marzo de 1997", *Sistema de Información Legal del Estado Plurinacional de Bolivia*, accedido 21 de septiembre de 2017, http://www.silep.gob.bo/silep/masterley/118557.
[1393] Presidencia del Estado Plurinacional de Bolivia, "Decreto Supremo N° 28168 de 17 de mayo de 2005", accedido 21 de septiembre de 2017, http://www.comunicacion.gob.bo/sites/default/files/docs/Decreto%20Supremo%20N%C2%BA%202816 8%20Acceso%20a%20la%20Informacion_0.pdf.
[1394] Congreso Nacional del Estado Plurinacional de Bolivia, "Ley 018, Ley del Órgano Electoral Plurinacional de Bolivia, de 16 de junio de 2010", *Sistema de Información Legal del Estado Plurinacional de Bolivia*, accedido 21 de septiembre de 2017, http://www.silep.gob.bo/silep/masterley/118207.

seguridad e integridad de la totalidad de la información registrada. De esta manera, se protegen los datos personales desde la perspectiva de los derechos a la intimidad y la privacidad.

- Ley 164, Ley General de Telecomunicaciones, Tecnologías de la Información y Comunicación, 8 de agosto de 2011, emitida por el Congreso Nacional del Estado Plurinacional de Bolivia,[1395] cuyo capítulo onceavo, denominado "Derechos y obligaciones de las usuarias y usuarios" de los servicios de telecomunicaciones y tecnologías de información y comunicación, en el artículo 54, numeral 9, declara el derecho a "Solicitar la exclusión, sin costo alguno, de las guías de usuarias o usuarios disponibles al público, ya sean impresas o electrónicas. Las usuarias o usuarios podrán decidir cuáles datos personales se incluyen, así como comprobarlos, corregirlos o suprimirlos". Su ámbito es sectorial, pero motiva el reglamento que se analiza a continuación en el cual existen varias referencias propias de la protección de datos personales. Finalmente, el artículo 84, numeral 3, determina que el reglamento referido a firmas y certificados digitales comprenderá "Las definiciones, principios y procedimientos relativos al tratamiento de los datos personales".

- Decreto Supremo 1793, que aprueba el Reglamento a la Ley 164, 8 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación.[1396]

Como en casos anteriores, para determinar el contenido esencial del derecho a la protección de datos en Bolivia, se acudirá a la normativa de aplicación general que, en este caso, es de orden constitucional; únicamente en aquellos casos que amerite se analizará la normativa secundaria, sectorial no generalmente aplicable.

a) Ámbito: Registros o ficheros públicos y privados

La norma constitucional determina, en el artículo 130, que el ámbito de aplicación de la acción de protección de privacidad son los archivos o bancos de datos públicos o privados.

b) Naturaleza del dato

El artículo 130 que describe la acción de protección a la privacidad reconoce como presupuesto de protección, los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados. Como se ve, esta aproximación general no determina la naturaleza del dato en sí mismo, tampoco se usa el término información, sino su forma de recogida y la identificación del soporte que la contiene. Por eso hay que acudir al Decreto Supremo 1793, que aprueba el Reglamento a la Ley 164, 8 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación (en adelante Decreto Supremo 1793). Allí, en el artículo

[1395] Congreso Nacional del Estado Plurinacional de Bolivia, "Ley 164, Ley General de telecomunicaciones, tecnologías de la información y comunicación, de 8 de agosto de 2011", *Sistema de Información Legal del Estado Plurinacional de Bolivia*, accedido 21 de septiembre de 2017, http://www.silep.gob.bo/silep/masterley/118680.

[1396] Presidencia del Estado Plurinacional de Bolivia, "Decreto Supremo No. 1793, que aprueba el Reglamento a la Ley No. 164, de 8 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación", *Gaceta Oficial del Estado Plurinacional de Bolivia*, accedido 21 de septiembre de 2017, http://www.cepb.org.bo/calypso/juridica/adjuntos/ds_1793.pdf.

3, relativo a las definiciones técnicas adopta varias, entre ellas la de datos personales, artículo 3, IV, a) señala que se entiende por datos personales a toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable. Su ámbito es sectorial por lo que no marca el contenido esencial del derecho, pero da cierta orientación.

Ahora bien, como en la norma constitucional no se consagra el derecho a la protección de datos personales, el dato aunque personal, para ser objeto de protección debe afectar derechos fundamentales como la intimidad y la privacidad personal o familiar, o a su propia imagen, honra y reputación y que no procederá para levantar el secreto en materia de prensa. En consecuencia, en Bolivia el dato personal debe ser íntimo, privado o afectar la imagen y la honra o reputación o algún otro derecho.

c) Sujeto activo

El citado artículo 130 de la Constitución boliviana señala, de forma general: toda persona individual o colectiva, de esta manera se incluye como titulares de esta acción constitucional, y por ende de los derechos que esta protege, tanto a personas naturales como a personas jurídicas. Lo que coincide con lo señalado en el artículo 3, IV, a) Decreto Supremo 1793, que determina que los datos personales serán aquella información concerniente a una persona natural o jurídica que la identifica o la hace identificable; nuevamente la norma es referencial para determinar el contenido esencial, pero brinda una guía.

d) Sujeto pasivo

El artículo 130 de la Constitución admite que la acción procede contra quien está a cargo de los archivos o bancos de datos, sean estos públicos o privados.

El Decreto Supremo 1793 señala que las entidades certificadoras (art. 39) son las que cumplirán con la recolección del consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales (art. 3, IV b)); así como respetarán los derechos fundamentales y garantías establecidas en la Constitución Política del Estado (art. 56).

e) Objeto o bien jurídico

a. Derecho de información

El artículo 130 de la Constitución determina que la acción de protección de privacidad protege a toda persona que haya sido indebida e ilegalmente impedida de conocer datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados. Dicho de otro modo, ante una obligación de entregar datos que afecten a las personas en sus derechos fundamentales como la intimidad, la privacidad personal o familiar, su propia imagen, honra y reputación, procede la acción de protección de privacidad, es decir, ante la negativa del responsable del fichero de informarlos. Llama la atención que la negativa del responsable del fichero puede estar justificada legalmente, puesto que la norma habla de que el impedimento no debe ser ilegal.

b. Autodeterminación informativa

Respecto de la autodeterminación informativa el artículo 130, se determina expresamente que la acción de protección de privacidad protege de aquella afectación a los derechos fundamentales a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación y que no procederá para levantar el secreto en materia de prensa. En consecuencia, en el texto constitucional boliviano no existe el derecho a la protección de datos personales como derecho autónomo e independiente.

Sin embargo, el Tribunal Constitucional reconoce este derecho a través de varias resoluciones entre las que se destaca la sentencia Constitucional 0030/2006-R de 11 de enero de 2006, que establece el que el ámbito de protección de la acción de privacidad es la autodeterminación informativa y por ende la dignidad de su titular:

> […] El hábeas data como una vía procesal instrumental de protección al derecho a la autodeterminación informativa, referido a los derechos fundamentales a la intimidad y la privacidad de la persona, fue incorporado al sistema constitucional boliviano mediante la Ley 2631 de Reforma de la Constitución de 20 de febrero de 2004». En el sistema constitucional boliviano, el hábeas data es una vía procesal instrumental para protección del derecho a la «autodeterminación informativa», precautelando que la persona pueda acceder al conocimiento de los datos o informaciones, referidos a su vida privada o íntima, así como la de su familia, obtenidos y almacenados en los bancos de datos públicos o privados, con la finalidad de conocer qué datos se han obtenido y almacenado; es decir, cuánta información, con qué finalidad y a quienes se distribuyó, se distribuye o distribuirá la misma.

En el mismo sentido, la autora Karina Medinaceli, respecto del reconocimiento a la autodeterminación informativa como derecho fundamental en Bolivia afirma que:

> […] la génesis constitucional del derecho a la «autotutela informativa» encuentra cauce jurídico en el bloque de constitucionalidad boliviano, específicamente en el art. 21.6 de la Constitución vigente; asimismo, su contenido se encuentra sustentado por los artículos 13 del Pacto de San José de Costa Rica, 19 de la Declaración Universal de los Derechos Humanos y 19.2 del Pacto Internacional de Derechos Civiles, adoptado por la Asamblea General de la Organización de Naciones Unidas; además es importante señalar también que este derecho encuentra fundamento en la Resolución 1932 de la Organización de Estados Americanos, adoptada en su sesión plenaria de 10 de junio de 2003, que por su naturaleza en el marco del artículo 41034 de la CPE, forma parte del Bloque de Constitucionalidad y que garantiza el libre acceso a la información de todo Estado Democrático. De lo expresado precedentemente, a partir del marco normativo descrito, se colige que el derecho a la «autotutela informativa», al margen de ser un derecho derivado, es también un derecho sustantivo, por tanto, en un Estado Social y Democrático de Derecho debe ser defendido por medios jurídicos idóneos, que logren su respeto efectivo[1397].

Es en este sentido que debe leerse la Ley 164, Ley General de Telecomunicaciones, Tecnologías de información y Comunicación en el artículo 56, sobre la inviolabilidad y secreto de las comunicaciones, señala que de conformidad con "lo establecido en la Constitución Política del Estado, los operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación deben

[1397] K. I. MEDINACELI, *El tratamiento de los datos sanitarios en la historia clínica electrónica: Caso boliviano* (Madrid: Agencia Española de Protección de Datos Personales, 2017), 212.

garantizar la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias o usuarios, salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma". Pues, aunque en dicha norma se distingue entre protección de datos personales y derecho a la intimidad en un análisis progresivo debe mirarse como separados e independientes estos dos derechos.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

No consta en la normativa referencia a este tema.

d. Principios

i. Deber de información

En la normativa constitucional no consta alusión a este principio. Únicamente en el artículo 30 de la Constitución aparece, de manera referencial, la negativa indebida e ilegal de dar a conocer datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, como se analizó en líneas anteriores cuando se habló del derecho de información.

Respecto al Decreto Supremo 1793, en el artículo 4, aplicable a quienes brinden servicios de certificación digital se establece el principio de transparencia, por el cual, cuando traten datos personales deberán garantizar al titular en cualquier momento y sin impedimento alguno la información relacionada de la existencia de los datos que le conciernan. Su aplicación es limitada a las entidades certificadoras; en este sentido este criterio sectorial es meramente orientativo.

ii. Pertinencia

No consta en la normativa constitucional boliviana referencia a este principio.

iii. Calidad

No consta en la normativa constitucional boliviana referencia a este principio. En cuanto al Decreto Supremo 1793, en el artículo 4, relativo a la obligatoriedad de quienes brinden servicios de certificación digital, cuando traten de datos personales deberán aplicar el principio de veracidad que se refiere a que la información sujeta a tratamiento debe ser veraz, completa, precisa, actualizada, verificable, inteligible, prohibiéndose el tratamiento de datos incompletos o que induzcan a errores. Es decir, se recogen aquellas características que definen al principio de calidad con otro nombre. Pese a su aplicación limitada, este sería el sentido aplicable a operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación.

iv. Finalidad

No consta en la normativa constitucional boliviana referencia a este principio. Sin embargo, el Decreto Supremo 1793, de aplicación limitada a operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, en el artículo 4, relativo a los principios que los servicios de certificación digital deben aplicar cuando traten de datos personales, señala que la

utilización y tratamiento de los datos personales por parte de las entidades certificadoras autorizadas, deben obedecer a un propósito legítimo, el cual debe ser de conocimiento previo del titular. De esta forma, se entiende para el contenido limitado de esta ley al principio de finalidad como aquel que justifica el tratamiento de datos únicamente si el propósito es legítimo.

Asimismo, en el artículo 56 del decreto citado consta que los titulares deberán ser informados previamente de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de estos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes. Los datos personales objeto de tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro. Nuevamente, este contenido es propio del principio de finalidad, sin embargo, el ámbito de aplicación de la ley es limitado a entidades certificadoras de firma digital.

v. Seguridad

No consta en la normativa constitucional boliviana referencia a este principio. El Decreto Supremo 1793, en el artículo 4, delimita entre los principios aplicables a las entidades certificadoras que traten datos personales, el de seguridad, por el cual en el tratamiento deberán implementar controles técnicos, administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento. Este criterio es referencial debido al ámbito limitado de aplicación del decreto.

vi. Consentimiento

No consta en la normativa constitucional boliviana referencia a este principio. Ahora bien, en el Decreto Supremo 1793, en el artículo 3, numeral IV, literal b), consta que el consentimiento será previo, expreso e informado del titular, por escrito u otro medio equiparable de acuerdo con las circunstancias; incluso podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo (art. 56) para llevar a cabo el tratamiento de datos personales por una entidad certificadora autorizada. Es decir, aquella que tiene por finalidad emitir, validar, renovar, denegar, suspender o dar de baja los certificados digitales; facilitar servicios de generación de firmas digitales; garantizar la validez de las firmas digitales, sus certificados digitales y la titularidad de su signatario; d) validar y comprobar cuando corresponda, la identidad y existencia real de la persona natural o jurídica; reconocer y validar los certificados digitales emitidos en el exterior; otras funciones relacionadas con la prestación de servicios de certificación digital (art. 39, Decreto Supremo 1793). En otras palabras, nuevamente el ámbito de aplicación limitado de este concepto de consentimiento no define el contenido esencial del derecho, pero da luces sobre él.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

a. Derecho de acceso

En la Constitución de 2009, en el artículo 130 está descrito solo de forma negativa el derecho de acceso, rectificación y eliminación, pues únicamente cuando los responsables de los ficheros impidan de forma ilegal o indebida estos derechos es posible que opere la acción de protección de la privacidad. Anotándose que también pueden eliminarse, rectificarse o acceder a datos siempre y cuando afecten los derechos fundamentales a la intimidad, privacidad, honra, propia imagen y buena reputación. Es decir, se requiere de presupuestos de ilegalidad y arbitrariedad para que la acción constitucional prospere. El sistema de protección no se basa ni en la titularidad del dato, ni en su consentimiento.

b. Derecho de rectificación

La norma citada (art. 130, Constitución boliviana 2009) menciona a la rectificación y, como se señaló anteriormente, esta solo prospera cuando de forma ilegal o indebida el responsable del fichero se niegue a rectificar la información o esta afecta derechos fundamentales.

c. Derecho de oposición

No consta referencia alguna al derecho de oposición.

d. Derecho de cancelación

Consta descrito como derecho de eliminación asociado únicamente cuando el responsable de una base de datos se niega de forma ilegal o indebida a eliminar datos, sobre todo si su permanencia afecta derechos fundamentales (art. 130, Constitución boliviana de 2009).

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

No existe referencia alguna a este derecho.

f. Derecho de consulta al registro general de protección de datos personales

No existe referencia alguna a este derecho.

g. Derecho a indemnización por daños causados

No existe referencia alguna a este derecho.

h. Derecho a la confidencialidad

No existe referencia alguna a este derecho en la Constitución boliviana de 2009. Sin embargo, en el Decreto Supremo 1793, relativo a las obligaciones de las entidades certificadoras, dispone en el artículo 4, el principio de confidencialidad por el cual todas "las personas involucradas y que intervengan en el tratamiento de datos personales, están obligadas a garantizar la reserva de la información, incluso hasta después de

finalizado su vínculo con alguna de las actividades que comprende el tratamiento, pudiendo únicamente realizar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las tareas autorizadas".

i. Derecho al olvido digital

No existe referencia alguna a este derecho.

j. Spam

En el Decreto Supremo 1793 en el título VI, sobre comunicaciones publicitarias, por medio de correo electrónico, en el Capítulo Único denominado "Comunicaciones comerciales publicitarias" consta el artículo 57, cuyo literal d) señala que las comunicaciones por medio de correo electrónico u otro medio de comunicación digital equivalente que tengan por finalidad la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional, deberán "indicar la forma, como el destinatario puede aceptar o rechazar el envío de futuras comunicaciones del remitente, para que los usuarios puedan habilitarse o deshabilitarse en el caso de que no deseen continuar recibiendo estos mensajes o correos". Asimismo, en el literal f) la necesidad de que la publicidad y acceso interactivo a los sitios web del proveedor a través de equipo terminal o "el simple registro comercial de ingreso no conlleva a un enlace comercial del proveedor que faculte difusión posterior, sino que ésta debe ser explícita y manifiestamente aceptada por suscripción" (art. 57, Decreto Supremo 1793).

g) Procedimiento

No existe procedimiento directo, solo acción constitucional descrita a continuación.

h) Acción de Protección de Privacidad (habeas data)

La Constitución Política del Estado de 1967 determinaba al *habeas data* como acción constitucional, posteriormente la vigente Constitución de 2009, en el capítulo segundo relativo a las acciones de defensa consagra la denominada Acción de Protección de Privacidad, constante en los artículos 130 y 131 con un contenido casi idéntico a su predecesora.

a. Sujeto activo

Se considera sujeto activo a toda persona natural y jurídica, aunque el artículo 130 de la Constitución menciona únicamente los términos "individual" y "colectiva", esta conclusión, que se puede obtener de una simple lectura progresista del texto constitucional, ha sido sustentada en la siguiente Jurisprudencia del Tribunal Constitucional establecida en la Sentencia Constitucional 965/2004-R que al respecto señala:

> […] La legitimación activa del hábeas data recae en la persona natural o jurídica –aunque el precepto constitucional no lo determina de esa manera en forma expresa, se entiende que dentro de la protección de este recurso se puede y debe abarcar tanto a las personas físicas como a las jurídicas, de quienes también se pueden registrar datos e informaciones– respecto de la cual la entidad pública o privada haya obtenido y tenga

> registrados datos e informaciones que le interesen a aquella conocer, aclarar, rectificar, modificar, o eliminar, y que no haya tenido respuesta favorable por la citada entidad para lograr esos extremos […]

Además, la misma sentencia analiza que serán las personas naturales o jurídicas individuales o colectivas incluso privados, los sujetos activos de este mecanismo constitucional, ya que como se refiere en el texto a continuación, a cada uno de ellos, en el caso que le corresponda, se le permitirá la defensa constitucional de los derechos que le corresponda:

> […] La nueva Constitución Política del Estado vigente cambia el nomen juris del hábeas data a Acción de Protección de Privacidad, pero no así su esencia tutelar, empero contempla algunos cambios específicos en cuanto a su redacción, en especial el art. 130.I, en el que se refiere a los casos de legitimación activa que si bien es muy similar al texto del art. 23.I de la abrogada CPE, tiene una diferencia notoria cuando afirma: «Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad». Se observa, en primer lugar, que se añaden a las personas colectivas como posibles legitimados activos, o futuros accionantes, concibiendo que las personas colectivas también tienen acceso a los derechos reconocidos por el art. 21.2 de la CPE, los cuales son: derecho a la intimidad, a la privacidad, honra, propia imagen y dignidad. Se entiende que el texto del artículo 130.I al reconocer como posibles accionantes a personas colectivas, se refiere a aquellas de orden público como privado, pero con algunas diferencias en cuanto a los derechos tutelados para estas, es decir, que las personas colectivas no podrán aducir la vulneración de su derecho a la intimidad personal y familiar, que son derechos fundamentales de índole personal, pero sí podrían denunciar la vulneración de sus derechos a la imagen y reputación. Corresponde aclarar que si bien el derecho a la imagen, a la honra y a la reputación, parecieran estar dentro del mismo grupo de derechos tutelados por la Acción de Protección de Privacidad, en el caso de las persona colectivas, que es el objeto del presente análisis, como se indica líneas supra, sólo podrían denunciar la vulneración de los derechos a la imagen y la reputación, pero no así de la honra, debido a que el derecho a la honra es de índole estrictamente personal, es decir, entra dentro de la esfera de la personalidad y es concebido doctrinalmente como la pretensión de respeto que corresponde a cada persona como reconocimiento de su dignidad frente a la sociedad (Sentencia Constitucional 1978/2011-R de fecha 7 de diciembre de 2011)[…]

Adicionalmente, el artículo 59 del Código Procesal Constitucional señala que la acción de protección de privacidad podrá ser interpuesta por:

> Toda persona natural o jurídica que crea estar afectada en su derecho, u otra persona a su nombre con poder suficiente; las herederas o herederos de una persona fallecida, que crean que ésta ha sido afectada en su derecho a la privacidad, imagen, honra y reputación, cuando dicho agravio genere directamente la vulneración de los derechos de ellas o ellos, en virtud del vínculo de parentesco con la difunta o difunto; la Defensoría del Pueblo y la Defensoría de la Niñez y Adolescencia.

b. Sujetos pasivos u obligados

El mismo artículo 130 de la Constitución señala que la acción procede contra quien está a cargo de los archivos o bancos de datos, sean estos públicos o privados.

Por su parte el artículo 60 del Código Procesal Constitucional determina que la acción de protección de privacidad podrá ser interpuesta contra: toda persona natural o jurídica responsable de los archivos o bancos de datos públicos o privados; toda persona natural o jurídica que pueda tener en su poder datos o documentos de cualquier naturaleza, que puedan afectar al derecho o la intimidad y privacidad personal, familiar o a la propia imagen, honra y reputación.

De este texto, es rescatable que se haya ampliado a cualquier tipo de datos la procedencia de la acción y no solo a aquellos considerados íntimos o privados, bastando que se transgredan cualquiera de los derechos citados. Se anota además que, la legitimación pasiva corresponde a cualquier persona natural o jurídica, pública o privada que compile datos personales en un registro, independientemente de la finalidad, incluida la comercial, pudiendo estar destinada únicamente a producir informes, aunque no los circule o difunda.

c. Derechos tutelados por la acción de protección de privacidad

Según el artículo 130 de la Constitución de 2009, los derechos tutelados por la acción de protección de privacidad son la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, y no procederá para levantar el secreto en materia de prensa. Esta concepción de la acción constitucional corresponde lo que en la doctrina se llama protección de primera generación.

Al respecto, la autora Karina Medinaceli señala que son diversos los derechos tutelados desde la acción de protección de privacidad, al tenor del siguiente análisis:

> […] por la forma de redacción de la norma constitucional, pareciera que la acción tutelar protege un solo derecho; o dicho desde otra perspectiva, pareciera que la intimidad y privacidad, la imagen, honra y reputación fuesen un solo derecho fundamental. Al respecto cabe aclarar que no se trata de un solo derecho fundamental, sino de diferentes derechos: a) El derecho a la intimidad y privacidad, […] b) El derecho a la imagen es la facultad o potestad que tiene toda persona de evitar la difusión incondicionada de su aspecto físico; c) El derecho a la honra y reputación […] Lo que sucede es que el Constituyente, al consagrar los derechos fundamentales en el catálogo de la Constitución, los ha consignado en un mismo numeral 2) del artículo 21, cual si se tratase de un solo derecho fundamental, cuando se trata de diferentes derechos, como se ha descrito precedentemente […] la protección a estos derechos está vinculada a la vulneración del derecho a la intimidad y privacidad en su dimensión positiva; lo que significa que no toda vulneración a los derechos a la imagen, la honra y la reputación activará la Acción de Protección de privacidad, sino que la misma tendrá lugar solamente en aquellos casos en los que, como consecuencia de la vulneración del derecho a la intimidad y privacidad en su dimensión positiva (derecho de autodeterminación informática) se vulneren esos derechos, causando daños y perjuicios a su titular o a su familia [...]

De lo transcrito podemos colegir que la acción de privacidad, no es equiparable al *habeas data*. Ya que, esta acción constitucional protege los datos personales como materialización de la autodeterminación informativa en cualquiera de sus formas, esto es a través de los derechos a la intimidad, a la privacidad, a la imagen, a la propia voz, a la honra, a la protección de datos personales. No se requiere entonces que el dato

personal que se cause un perjuicio sea íntimo o privado, por ende debería ser posible que ante cualquier ataque a la dignidad humana evidenciado en la transgresión de cualquiera de estos derechos a través de un dato personal pudiera ser tutelado efectivamente. La intimidad y la privacidad no pueden convertirse en un prerrequisito o condicionante previo que debe cumplirse para habilitar la interposición del *habeas data*. En este sentido, la consagración de la acción de protección de la privacidad en la vigente Constitución boliviana sería un retroceso, tanto más que la versión constitucional anterior si constaba reconocido directamente al *habeas data*.

Por su parte, el artículo 58 de la Código Procesal Constitucional, 5 de julio de 2012 señala que la Acción de Protección de Privacidad tiene por objeto:

> […] garantizar el derecho de toda persona a conocer sus datos registrados por cualquier medio físico, electrónico, magnético o informático, que se encuentre en archivos o bancos de datos públicos o privados; y a objetar u obtener la eliminación o rectificación de éstos cuando contengan errores o afecten a su derecho a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación.

Es decir, no se reconoce a la autodeterminación informativa ni a la protección de datos personales en el enunciado de derechos que serán protegidos a través de esta garantía, pero de la redacción se establece que la imagen, la honra y la reputación no necesitan que los datos sean íntimos o privados para que proceda esta acción.

Adicionalmente, Medinaceli sostiene que la Acción de Protección de Privacidad tutela o protege el derecho a la intimidad y privacidad en su dimensión positiva, esto es la de acceder a la información íntima o privada de un titular en distintas bases de datos públicas o privadas y no en cuanto a su enfoque negativo es decir no se protege el derecho a la inviolabilidad de domicilio, la inviolabilidad de comunicaciones privadas, y la inviolabilidad de documentos privados.

Asimismo, la Jurisprudencia dictada por el Tribunal Constitucional a través de la Sentencia Constitucional 0965/2004-R de 23 de junio de 2004 añade como parte de los derechos tutelados mediante la acción de protección de la privacidad, el de actualización:

> […] b) Derecho a la actualización de la información o los datos personales registrados en el banco de datos, añadiendo los datos omitidos o actualizando los datos atrasados; con la finalidad de evitar el uso o distribución de una información inadecuada, incorrecta o imprecisa que podría ocasionar graves daños y perjuicios a la persona[…]

Por su parte, la Jurisprudencia del Tribunal Constitucional en sentencia No. 0965/2004-R de 23 de junio de 2004, establece otro derecho el de confidencialidad:

> […] d) Derecho a la confidencialidad de cierta información legalmente obtenida, pero que no debería trascender a terceros porque su difusión podría causar daños y perjuicios a la persona […]

Finalmente, la Jurisprudencia del Tribunal Constitucional a través de la Sentencia Constitucional 0965/2004-R de 23 de junio de 2004, reconoce sobre los datos sensibles lo siguiente:

> […] e) Derecho de exclusión de la llamada «información sensible» relacionada al ámbito de la intimidad de la persona, es decir, aquellos datos mediante los cuales se pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como las ideas religiosas, políticas o gremiales, comportamiento sexual; información que potencialmente podría generar discriminación o que podría romper la privacidad del registrado».

De lo dicho, queda claro que será el Tribunal constitucional boliviano el que irá definiendo el alcance de la acción de protección de privacidad y los derechos tutelados a través de él.

d. Procedencia

Conforme señala el citado artículo 130 de la Constitución de 2009, procede cuando es indebida o ilegal la negativa del que tenga los archivos o las bases de datos públicas o privadas de dar a conocer, objetar u obtener la eliminación o rectificación de los datos registrados.

El artículo 62 del citado Código Procesal Constitucional señala que esta acción no procederá en los siguientes casos: cuando se haya interpuesto para levantar un secreto en materia de prensa; cuando hayan cesado los efectos del acto reclamado; cuando se refiera a una resolución administrativa cuya ejecución estuviere suspendida por efecto de algún medio de defensa o recurso; constituyan actos consentidos libre y expresamente; o resoluciones judiciales o administrativas que pudieran ser modificadas o suprimidas por cualquier recurso.

e. Procedimiento

Conforme señala el artículo 131 de la Constitución de 2009 el procedimiento de la Acción de Protección de Privacidad era el mismo previsto para la acción de Amparo Constitucional. Es decir, si el tribunal o juez competente declaraba procedente la acción, ordenaba al administrador de la base de datos públicos o privados, la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado. Esa decisión podía elevarse, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución. La decisión final que concedía la acción de protección de privacidad, era ejecutada inmediatamente y sin observación alguna por parte del administrador de la base.

A partir de la promulgación del Código Procesal Constitucional de fecha 5 de julio de 2012, se establece un procedimiento específico para la Acción de Protección de Privacidad, por lo cual ya no debe usarse el procedimiento de la Acción de Amparo Constitucional como lo establecían la Constitución Política del Estado de 1967 (art. 23, parágrafo V) y la Constitución de 2009 (art. 131.I).

El artículo 61 Código Procesal Constitucional señala que la acción de protección de privacidad "podrá interponerse de forma directa, sin necesidad de reclamo administrativo previo, por la inminencia de la violación del derecho tutelado y la acción tenga un sentido eminentemente cautelar". Una vía directa de reclamo, facilita el ejercicio de la acción, tanto más que no se requiere de una negativa u omisión de respuesta del responsable del tratamiento para que se viabilice la interposición de la acción.

Conforme señala el artículo 63 del Código en mención, los efectos de una resolución que otorgue al peticionario la protección de su privacidad serán: establecer la existencia de indicios de responsabilidad civil o penal; la revelación de los datos cuyo registro fuera impugnado; se admita la objeción del accionante; o la eliminación o rectificación de los datos del accionante.

i) Institucionalidad de protección

No existe referencia sobre la institucionalidad de protección.

j) Régimen sancionador

No existe referencia sobre el régimen sancionador; sin embargo, el artículo 31 de la norma constitucional señala que en caso de resistencia a la revelación, eliminación o rectificación de datos impugnados se procederá de acuerdo con lo señalado en la Acción de Libertad. Esto es, de conformidad con el artículo 127: los servidores públicos o personas particulares que resistan las decisiones judiciales en los casos previstos por esta acción, serán remitidos por orden de la autoridad que conoció de la acción ante el Ministerio Público para su procesamiento penal por atentado contra las garantías constitucionales.

Finalmente, en el caso de que la autoridad judicial que no proceda a cumplir con la remisión al Ministerio Público podrá ser sancionada, penal, civil o administrativamente de conformidad con la Constitución y la ley.

k) Transferencia internacional de datos

No existe referencia sobre transferencia internacional de datos.

2.11 Panamá (2002)

La primera forma de reconocimiento del acceso a la información personal, se produce mediante la Ley 6, 22 de enero de 2002, Transparencia y Acceso Información Pública, que establece la acción de *habeas data* (arts. 3, 13 y 17).[1398]

Posteriormente, la Constitución Política de la República de 1972 ha tenido varias modificaciones en los años 1978, 1983, 1994 y 2004. En la última modificación, se incorporó en un Texto Único, publicado en la Gaceta Oficial 25176, la versión final que reconoce por primera vez, a nivel constitucional, el derecho de acceso a la información pública, el acceso a información de carácter personal, y la acción constitucional de *habeas data*.

Respecto del derecho de acceso a información de carácter personal la normativa expresamente señala:

[1398] Asamblea Legislativa de la República de Panamá, "Ley N° 6, de 22 de enero de 2002, que dicta normas para la transparencia en la gestión pública, establece la acción de *habeas data*, y dicta otras disposiciones", *Legispan, Legislación de la República de Panamá*, accedido 22 de noviembre de 2017, http://www.asamblea.gob.pa/legispan-2/.

> Artículo 42. Toda persona tiene derecho a acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley.
>
> Esta información sólo podrá ser recogida para fines específicos, mediante consentimiento de su titular o por disposición de autoridad competente con fundamento en lo previsto en la Ley.[1399]

Asimismo, las reformas constitucionales del 2004 incluyen el derecho de acceso a la información pública al tenor de lo siguiente:

> Artículo 43. Toda persona tiene derecho a solicitar información de acceso público o de interés colectivo que repose en bases de datos o registros a cargo de servidores públicos o de personas privadas que presten servicios públicos, siempre que ese acceso no haya sido limitado por disposición escrita y por mandato de la Ley, así como para exigir su tratamiento leal y rectificación.[1400]

Finalmente, el *habeas data* se encuentra reconocido en el artículo 44 de la Constitución reformada en el año 2004; textualmente dice:

> Artículo 44. Toda persona podrá promover acción de hábeas data con miras a garantizar el derecho de acceso a su información personal recabada en bancos de datos o registros oficiales o particulares, cuando estos últimos traten de empresas que prestan un servicio al público o se dediquen a suministrar información.
>
> Esta acción se podrá interponer, de igual forma, para hacer valer el derecho de acceso a la información pública o de acceso libre, de conformidad con lo establecido en esta Constitución.
>
> Mediante la acción de hábeas data se podrá solicitar que se corrija, actualice, rectifique, suprima o se mantenga en confidencialidad la información o datos que tengan carácter personal.
>
> La Ley reglamentará lo referente a los tribunales competentes para conocer del hábeas data, que se sustanciará mediante proceso sumario y sin necesidad de apoderado judicial.[1401]

La Constitución Panameña de 2004 incorpora el derecho de acceso a datos vinculados al individuo, y además la garantía constitucional del *habeas data*. En conjunto, esta forma de reconocimiento entre derecho y garantía significa que el derecho a la autodeterminación informativa, se encuentra vigente en la normativa panameña. Es decir, se otorga a las personas derechos como el de acceso, rectificación, cancelación y oposición respecto del tratamiento de sus datos personales que son parte del contenido esencial del derecho a la protección de datos personales.

Ahora bien, para que este derecho, reconocido constitucionalmente, se aplique de manera efectiva es necesario una normativa legal de carácter general que lo regule

[1399] Asamblea Nacional de la República de Panamá, "Constitución Política de la República de Panamá", *Political Database of the Americas*, accedido 22 de noviembre de 2017, http://pdba.georgetown.edu/Constitutions/Panama/vigente.pdf.
[1400] Ibíd.
[1401] Ibíd.

específicamente, que desarrolle, el ámbito de aplicación; los criterios de licitud del tratamiento; los principios: finalidad, calidad de datos, medidas de seguridad, entre otros; las obligaciones de los responsables de tratamiento; las infracciones y sanciones; y, la autoridad de control que supervigile el cumplimiento de la normativa.

Por lo tanto, para febrero de 2017, el Poder Ejecutivo presentó el proyecto de ley número 665 sobre datos personales. Para el 24 de octubre del 2018, la Asamblea Nacional aprobó en tercer debate un texto consensuado entre diversos actores. Posteriormente, el 26 de mayo de 2019, el Presidente de la República sancionó el texto y promulgó la Ley 81, de 26 de mayo de 2019, Ley de Protección de Datos Personales de Panamá,[1402]en adelante Ley 81.

Además, existe normativa de carácter sectorial que también es aplicable a la temática. Tal como se ha realizado en análisis anteriores solo se utilizará esta regulación dispersa en el caso de que pueda ser usada como criterio orientador para determinar el contenido esencial:

- Ley 3, 5 de enero de 2000, Ley General sobre las Infecciones de Transmisión Sexual, el Virus de la Inmunodeficiencia Humana y el Sida (art. 34).[1403]
- Ley 6, 22 de enero de 2002, que dicta normas para la transparencia en la gestión pública, establece la acción de *habeas data* y expide otras disposiciones.
- Decreto Ejecutivo 124, 21 de mayo de 2002, por la cual se reglamenta la Ley 6, 22 de enero de 2002.[1404]
- Ley 24, 22 de mayo de 2002, que regula el servicio de información sobre el historial de crédito; modificada por la Ley 14 de 2006 y la Ley 135, de 2013.[1405]

a) Ámbito: Registros o ficheros públicos y privados

Tanto en el artículo 42 como en el 44 de la Constitución Panameña, derecho y garantía, respectivamente, las bases de datos o registros a los que las personas tienen derecho a acceder son de carácter público (oficiales) y privado (particulares).

En el texto del citado artículo 44 existe una imprecisión, ya que cuando se señala que la acción de *habeas data* permite el acceso a información personal únicamente cuando esta se encuentre contenida en bancos de datos o registros oficiales o particulares de empresas que prestan un servicio al público o se dediquen a suministrar información. Por lo que, aquellas entidades privadas que no tienen por finalidad entregar información quedaban fuera del ámbito de aplicación. Este error conceptual, es corregido en la Ley

[1402] Asamblea Nacional de la República de Panamá, "Ley 81, de 26 de mayo de 2019, sobre Protección de Datos Personales", *Gaceta Oficial Digital*, accedido el 28 de agosto de 2019, https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf

[1403] "Ley No. 3 del 5 de enero de 2000, Ley General sobre las Infecciones de Transmisión Sexual, el Virus de la Inmunodeficiencia Humana y el Sida", *Legispan, Legislación de la República de Panamá*, accedido 22 noviembre 2017, en http://www.asamblea.gob.pa/legispan-2/.

[1404] Ministerio de Gobierno y Justicia de la República de Panamá, "Decreto Ejecutivo 124, 21 de mayo de 2002, por la cual se reglamenta la Ley 6, 22 de enero de 2002", *Justia Panamá*, accedido 30 de diciembre de 2017, https://docs.panama.justia.com/federales/decretos-ejecutivos/124-de-2002-may-22-2002.pdf.

[1405] Asamblea NACIONAL DE PANAMÁ, "Ley 24, 22 de mayo de 2002, que regula el servicio de información sobre el historial de crédito, modificada por la Ley 14 de 2006 y la Ley 135 de 2013", *Legispan, Legislación de la República de Panamá*, accedido 22 de noviembre de 2017, http://www.asamblea.gob.pa/legispan-2/.

81, ya que el derecho a la protección de datos personales debe ser protegido independientemente de la razón social de la entidad responsable de la base de datos, pues el elemento vinculante es el registro de datos personales con fines distintos a los domésticos. Por ello, el artículo 1 de la Ley 81 corrige este problema, pues el vigente texto amplía el ámbito de aplicación a cualquier tipo de entidad, ya que estipula que "toda persona, natural o jurídica, de derecho público o privado, lucrativa o no, puede efectuar el tratamiento de datos personales, siempre que lo haga con arreglo a la presente Ley y para los fines permitidos en el ordenamiento jurídico".

b) Naturaleza del dato

Los artículos 42 y 44 de la Constitución panameña, únicamente referencian la frase "información personal contenida en bases de datos o registros" sin mayores elementos aclaratorios. No determina definición alguna, únicamente hace alusión a que son datos de *carácter personal*.

Ahora bien, la Ley 81 señala en su artículo 4 la definición de dato personal que es cualquier información concerniente a personales naturales, que las identifica o las hace identificables. De esta manera, este concepto coincide con el estándar internacional. Anotándose que hace referencia expresa a datos de personas naturales, por lo que estos serán los únicos titulares del derecho, excluyendo de esta forma a las personas jurídicas.

La citada norma en su numeral 2, al definir base de datos como el conjunto ordenado de datos de "cualquier naturaleza, cualquiera que sea la forma o modalidad de su creación, organización o almacenamiento, que permite relacionar los datos entre sí", nos aclara además que el ámbito de protección de esta norma son los datos en cualquier tipo de soporte sea físico o electrónico. Respecto de tratamiento de datos, el numeral 20 del artículo 4, determina que es "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permita recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, asociar, disociar, comunicar, ceder, intercambiar, transferir, transmitir o cancelar datos, o utilizarlos en cualquier otra forma".

El citado artículo 4 de la Ley 81 establece como una de las categorías de datos personales, a los sensibles, que serán aquellos regulados que identifiquen de manera unívoca a una persona natural y que se refieren "a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este". Además, enuncia aquellos datos que deben ser considerados sensibles, que serán los que puedan revelar aspectos como "origen racial o étnico; creencias o convicciones religiosa, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, a la preferencia u orientación sexual, datos genéticos o datos biométricos, entre otros".

Respecto de este tipo de datos, el artículo 13 señala que los datos sensibles no pueden ser objeto de transferencia, excepto cuando: el titular haya dado su autorización explícita; sea necesario para salvaguardar la vida del titular; se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; tenga una finalidad histórica, estadística o científica, siempre que se disocien;

Artículo 20. Los establecimientos de salud públicos o privados y los profesionales de la medicina puedan recolectar y procesar los datos personales relativos a la salud física o mental de los titulares que como pacientes acudan a estos o que estén o hubieran estado bajo su tratamiento, respetando los principios de secreto profesional y lo establecido en la presente Ley o leyes especiales que regulan dicha materia.

Además, el numeral 6 del citado artículo 4 de ley 81, distingue a los datos confidenciales, como aquellos que "por su naturaleza no deben ser de conocimiento público o de terceros no autorizados, incluyendo aquellos que estén protegidos por ley, por acuerdos de confidencialidad o de no divulgación", y por ende serán de acceso restringido. En este concepto destacan los datos personales que trata la Administración Publica, que serán confidenciales para el tratamiento limitado a los fines de la Administración, sin perjuicio de lo dispuesto por leyes especiales.

No serán del ámbito de aplicación de esta norma los datos anónimos, que son aquellos "cuya identidad no puede ser establecida por medios razonables o el nexo entre este y la persona natural a la que refiere". Por su parte, tampoco lo será, el dato disociado, que es aquel que "no puede asociarse al titular ni permitir por su estructura, contenido o grado de desagregación la identificación de la persona sea esta natural". La normativa reconoce también a los procedimientos de disociación o anonimización, entendidos como "todo tratamiento de datos que impide que la información disponible en la base de datos pueda asociarse a persona natural determinada o determinable". Respecto de estos procedimientos, suelen exigir reparos debido al avance tecnológico que permite mecanismos de reversión por los cuales data anónima pueden volverse dato personal, más aun data disociada sometida a un tratamiento inverso puede volverse nuevamente identificable.

El artículo 4 numeral 14 de la Ley, destaca el concepto de fuente accesible, comprendida como aquellas bases de datos que no son de acceso restringido o tengan reserva alguna a consultas, por lo que serán aquellas de acceso público como:

> las publicaciones estatales de carácter oficial, los medios de comunicación, los directorios telefónicos y la lista de personas que pertenecen a un grupo de profesionales que contengan únicamente nombre, titulo o profesión, actividad, dirección laboral o comercial, al igual que información que indique su pertenencia a organismos.

La Ley 6, 22 de enero de 2002, cuyo limitado campo de aplicación es el sector público para temas de transparencia en la gestión pública, determina en el artículo 1, numeral 4, que se deberá entender como información todo tipo de datos contenidos en cualquier medio, documento o registro impreso, óptico, electrónico; químico, físico o biológico. El citado artículo en los numerales 5, 6 y 7 también establece otras categorizaciones: a) información confidencial, es decir, aquella que si bien consta en manos del Estado o de cualquier institución pública es íntima o es relativa a correspondencia o comunicación telefónica; así como información de funcionarios de su expediente de recursos humanos y que no podrá ser divulgada bajo ninguna circunstancia e incluso en procesos judiciales deberá constar como reservada (art. 13); b) información de acceso libre, aquella que no tiene restricción; c) Información de acceso restringido, por la cual toda información que está en manos de agentes del Estado o cualquier institución pública, cuya divulgación ha sido circunscrita exclusivamente a funcionarios que deban conocerla en ejercicio de sus atribuciones de acuerdo con la ley.

c) Sujeto activo

Cuando el artículo 42 de la Constitución panameña consagra el derecho, determina de forma general a los titulares al señalar que será toda persona. Ahora bien, es nuevamente en la Ley 6, 22 de enero de 2002, sobre *habeas data* en el artículo 1, numeral 9, que se aclara que son titulares también las personas jurídicas que actúen a nombre propio o incluso de un tercero.

Sin embargo, la Ley 81 determina en el artículo 4 que para efectos de esta Ley, se considerará titular de los datos únicamente a la persona natural a la que se refieren los datos, dejando de lado a las personas morales. Enfoque que coincide con el concepto de dato personal previsto en el artículo 4 de la cita ley, cuando señala que se considera dato personal a cualquier información concerniente a personales naturales.

d) Sujeto pasivo

Acerca del derecho a la protección de datos, aunque no existe mención expresa en la norma constitucional, artículo 42, respecto de quienes son los sujetos pasivos, estos pueden ser deducidos de su simple lectura, estos son los responsables de las bases de datos o registros públicos y privados.

Por su parte, el artículo 4 de la Ley 81 señala dos tipos de sujetos pasivos:

- *Responsable del tratamiento de los datos*: Es la "persona natural o jurídica, de derecho público o privado, lucrativa o no, que le corresponde las decisiones relacionadas con el tratamiento de los datos y que determina los fines, medios y alcance, así como cuestiones relacionadas a estos", numeral 17. Este concepto coincide tanto en denominación como en contenido con el estándar internacional, puesto que será aquel a quien se le atribuye responsabilidad directa respecto de las directrices de tratamiento que tome respecto de los datos personales a su cargo y que puede encargar al custodio a actuar pos su cuenta.

- *Custodio de la base de datos* es la "persona natural o jurídica, de derecho público o privado, lucrativa o no, que actúa a nombre y por cuenta del responsable del tratamiento y le compete la custodia y conservación de la base datos", numeral 5. Este concepto coincide con el establecido a nivel general como encargado, que no tiene responsabilidad directa a menos que no acate las directrices emitidas por el responsable, aunque en esta definición se le asigna obligación sobre la custodia y conservación de los datos.

e) Objeto o bien jurídico:

a. Derecho de información

No consta establecido como derecho de información sino como principio de transparencia conforme dispone el artículo 2 de la Ley 81.

b. Autodeterminación informativa

No consta en la normativa constitucional ni legal panameña referencia expresa a este derecho. Sin embargo, al reconocer la Constitución Panameña de 2004 el derecho de acceso a datos vinculados al individuo, y el *habeas data*, se colige que se ha reconocido a la autodeterminación informativa contenido esencial del derecho a la protección de datos personales. Tanto más que, a través del *habeas data*, el titular no solo tiene derecho de acceso sino también de rectificación, cancelación y oposición.

Es a través de la Ley 81 que se efectiviza el derecho a la protección de datos personales y por ende se reconoce la autodeterminación informativa al otorgar al titular derechos como el de acceso, rectificación, cancelación y oposición, artículo 15 de la citada Ley. Ya que, a través de estos derechos, el titular puede decidir sobre quién, cómo, en qué contextos, con qué finalidades, por cuánto tiempo un responsable de tratamiento puede tratar sus datos personales.

El artículo 1 de la mencionada norma señala que, el titular ejerce pleno ejercicio de sus derechos fundamentales "considerando su interrelación con la vida privada y demás derechos y libertades fundamentales de los ciudadanos". Redacción que permite colegir que un inadecuado tratamiento de los datos personales no solo afecta a la intimidad sino que la información personal, al ser parte de la dignidad humana, guarda estrecha relación con otros derechos fundamentales, sobre todo aquellos relacionados con la personalidad, que pueden ser transgredidos por los desarrollos tecnológicos.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

El artículo 42 de la Constitución panameña señala que toda persona tiene derecho a acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la ley. Esta información solo podrá ser recogida para fines específicos, mediante consentimiento de su titular o por disposición de autoridad competente con fundamento en lo previsto en la ley.

De la transcripción realizada se desprende que existe necesidad de mandato legal para realizar tratamiento de datos personales cuando no media consentimiento del titular del dato, pero se añade que no es la ley de forma automática, sino que necesita de la disposición de una autoridad competente que interprete la ley.

Pese al texto constitucional, es precisamente la Ley 81 la que establece en su artículo 6, la licitud del tratamiento, es decir, sin necesidad de pronunciamiento de una autoridad, sino por la sola disposición de la ley, es posible el tratamiento de datos personales por parte de un responsable cuando se cumplan al menos una de las condiciones siguientes: mediante consentimiento del titular; necesario para ejecución de una obligación contractual; necesario para el cumplimiento de una obligación legal; o, autorizado por una ley especial.

Finalmente, en el ámbito de exclusión, es decir, cuando no es aplicable esta normativa de protección de datos, el artículo 3 de la Ley 81 dispone que: "se exceptúan del ámbito de esta Ley aquellos tratamientos que expresamente se encuentran regulados por leyes especiales o por las normativas que las desarrollen, además de los tratamientos de datos

personales siguientes: los que realice una persona natural para actividades exclusivamente personales o domésticas; los que realicen autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales; los que se efectúen para el análisis de inteligencia financiera y relativos a la seguridad nacional; el tratamiento de datos relaciones con organismos internacionales; o, los resultantes de un procedimiento previo de disociación o anonimización".

En el ámbito de aplicación territorial de la Ley 81, el artículo 5 dispone que sea aplicable a las bases de datos que se encuentren en el territorio panameño, ya sea que los datos personales sean de nacionales o extranjeros o que el responsable del tratamiento de los datos esté domiciliado en el país. Se excluye la base datos de sujetos regulados por leyes especiales.

d. Principios

i. Deber de información o transparencia

El artículo 2 de la Ley 81, conceptualiza el principio de transparencia que es aquel equiparable con el deber de información ya que determina que:

> […] toda información o comunicación al titular de los datos personales relativa al tratamiento de estos deberá ser en leguaje sencillo y claro, y mantenerlo informado de todos los derechos que le amparan como titular del dato, así como la posibilidad de ejercer los derechos ARCO.

Coincide con este texto, lo dispuesto en el artículo 6 de la Ley 81 que establece como elemento condicional para que el consentimiento sea efectivo que, la persona sea "debidamente informada respecto del propósito del uso de sus personales".

De lo transcrito se puede colegir que, el principio de transparencia en la normativa panameña se limita a informar al titular sobre derechos Arco y sobre la finalidad con la que se usarán sus datos, cuando, conforme establece el estándar europeo, el deber de información del responsable de tratamiento está asociado a otros principios como el de calidad, proporcionalidad, lealtad, minimización; a otros derechos como el de portabilidad; así como, a la cesión de datos, procedimientos, e identidad de los responsables de tratamiento, de oficiales de cumplimiento, o de autoridades, entre otros.

En suma, una adecuada redacción sobre el principio de información o de transparencia hace alusión a todas aquellas relaciones de lealtad que deben existir entre titulares, responsables y autoridad para que los principios, derechos y obligaciones puedan ser ejercidos con conocimiento suficiente y por ende, de forma efectiva y eficiente.

ii. Pertinencia

El artículo 2 de la Ley 81 que dispone los principios generales que rigen a la protección de datos de carácter personal no consta el de pertinencia, su contenido está referenciado en el principio de proporcionalidad, de calidad y en el de finalidad como veremos a continuación.

iii. Calidad

El artículo 2 de la Ley 81 señala el principio de veracidad y exactitud, entendido como aquel por el cual los datos de carácter personal "serán exactos y puestos al día de manera que respondan con veracidad a la situación actual del propietario del dato".

En este concepto se hace alusión específica a la necesidad de actualidad del dato que permite la veracidad y la exactitud del mismo, sin embargo estas características no provienen exclusivamente de la vigencia del dato sino que deben ser el reflejo de la realidad.

iv. Finalidad

Tal como señala el texto del artículo 42 de la Constitución panameña, la información personal solo podrá ser recogida para fines específicos, mediante consentimiento de su titular o por disposición de autoridad competente con fundamento en lo previsto en la ley. De esa forma, la finalidad es fundamental aun cuando haya consentimiento o incluso mandato de autoridad competente.

Ahora bien, el artículo 2 de la Ley 81 estipula que el principio de finalidad es aquel por el cual los datos personales "deben ser recolectados con fines determinados y no ser tratados posteriormente para fines incompatibles o distintos para los que se solicitaron, ni conservar por tiempo mayor del necesario para los fines de tratamiento". La finalidad requiere la determinación previa del uso que se dará a los datos personales, de tal manera que se evidencia la pertinencia entre los datos solicitados, la finalidad declarada y el efectivo tratamiento de datos personales realizado.

Asimismo, el artículo 11 de la Ley 81 señala que los datos personales deben utilizarse para los fines determinados, explícitos y lícitos para los cuales hubieran sido autorizados al momento de su recolección. En este sentido la finalidad, está directamente referenciada a la licitud del tratamiento y al deber de información por el cual el titular conoce de manera explícita con qué fin se tratarán sus datos personales.

No se incluye en esta normativa la alusión expresa de que la finalidad puede cambiar posteriormente, sino que menciona de manera general que la finalidad puede cambiar por cualquier motivo, de tal manera que otro uso requerirá de la revisión de la licitud de su tratamiento, es decir verificar si existe normativa que habilite el tratamiento, necesidad del cumplimiento de una obligación contractual o legal, incluida las competencias públicas y de ser el caso, solicitarse el consentimiento del titular para la nueva finalidad.

v. Seguridad

Al tenor de lo señalado en el artículo 2 de la Ley 81, el principio de seguridad de los datos dispone que los responsables del tratamiento de los datos personales deban:

> […] adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos bajo su custodia, principalmente cuando se trate de datos considerados sensibles, e informar al titular, lo más pronto posible, cuando los datos

> hayan sido sustraídos sin autorización o haya indicios suficientes de que su seguridad ha sido vulnerada.

Del texto se colige que, la seguridad no solo referencia a medidas técnicas sino también organizativas, pero además, establece un deber de información, por parte del responsable de tratamiento que está obligado a notificar al titular de la sustracción de sus datos o de la vulneración de la seguridad. Todo ello con la finalidad de que, el titular pueda arbitrar medidas de protección que mitiguen posibles daños ocurridos por las fugas de información.

Niveles de seguridad, esto es, medidas técnicas y de gestión adecuada para preservar la seguridad en la explotación de la red o en la presentación de los servicios, así como el cumplimiento de certificaciones, protocolos, estándares y otras medidas que establezcan las autoridades respectivas, también le son exigidos a los operadores que gestionen redes públicas o que presten servicios de comunicación disponibles al público, artículo 26 de la Ley 81. Esta norma está direccionada a los proveedores de servicios de internet, y es necesaria no por la condición de tratante de datos personales, sino porque a través de su infraestructura corre todo el tráfico de datos, incluidos los personales.

En caso de vulneraciones también están obligados a informar a los titulares sobre dicha afectación y sobre las medidas a adoptar. Anotándose que, esta regulación se entiende sin perjuicio de lo previsto en las normas especiales sobre telecomunicaciones, relacionadas con la seguridad pública y la defensa nacional, artículo 26 citado.

vi. Consentimiento

El artículo 42 de la Constitución panameña señala que para el registro de información personal en bases de datos o registros públicos y privados será necesario el consentimiento del titular del dato. El numeral 8 del artículo 2 de la Ley 81 establece que para que exista licitud en el tratamiento de un dato personal, este deberá ser "recolectado y tratado con el consentimiento previo, informado e inequívoco del titular del dato o por fundamento legal". De esta forma, el texto constitucional coincide con lo dispuesto en la Ley de Protección de Datos, estableciendo al consentimiento como una de las condiciones más importantes que viabilizan un tratamiento adecuado de los datos personales. De tal manera, el consentimiento es una de las condiciones de licitud del tratamiento y no como derecho de un titular, conforme la normativa panameña.

El numeral 4 del artículo 4 de la Ley 81, al definir consentimiento señala que es "la manifestación de la voluntad del titular de los datos, mediante la cual se efectúa el tratamiento de estos".

La voluntad puede ser emitida de forma directa o a través de mandato, pero el mandatario deberá respetar lo estipulado por el titular y se dejará constancia, por escrito o de forma electrónica, con la condición de que pueda demostrarse con certeza su otorgamiento y las condiciones para el tratamiento o utilización, y conforme el artículo 10 de la Ley.

El artículo 6 de la Ley 81, determina que el consentimiento debe mantener su "trazabilidad mediante documentación, ya se electrónica o mediante cualquier otro

mecanismo que resulte adecuado al medio de que se trate el caso". Además, el consentimiento podrá ser revocado, sin efecto retroactivo.

El artículo 8 de la Ley 81 señala cuando no se requiere autorización para el tratamiento de datos personales. El numeral 4 del artículo 6, establece que es posible tratar datos por autorización de su titular o por autorización de la ley, de tal manera que, los casos enunciados en esta norma no son más que mandatos legales autorizando dicho tratamiento.

En consecuencia, al tenor del citado artículo 8 de la Ley 81, no se requiere de autorización para el tratamiento de datos personales cuando estos: provengan o que se recolecten de fuentes de dominio público o accesible en medios públicos; para el ejercicio de competencias de la Administración Pública; los de carácter económico, financiero, bancario o comercial que cuenten con el consentimiento previo; que se contengan en listas relativas que se limiten a indicar la pertenencia de la persona natural a una organización, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento; los necesarios dentro de una relación comercial establecida; el que realicen organizaciones privadas para el uso exclusivo de sus asociados y de las entidades afiliadas; los casos de urgencia médica o sanitaria, (cuando el consentimiento se refiera a datos personales sensibles de salud, el consentimiento será previo, irrefutable y expreso); para fines históricos, estadísticos o científicos, siempre que estos sean anonimizados por el responsable de su custodia o tratamiento (art. 12); satisfacción de intereses legítimos, siempre que sobre dichos intereses no prevalezcan derechos del interesado, en particular cuando el interesado sea un menor de edad o persona con discapacidad.

Respecto del consentimiento para la cesión, los responsables del tratamiento de datos solo podrán transferir información sobre estos cuando cuenten con el consentimiento previo, informado e inequívoco del titular, salvo las excepciones establecidas en esta Ley o en las leyes especiales. Si el consentimiento se da en una declaración que se refiera a otros asuntos, se presentará de tal forma que se distinga claramente, forma comprensible y de fácil acceso utilizando un lenguaje claro y sencillo, al tenor de lo señalado en el artículo 25 de la Ley 81.

vii. Lealtad

Conforme el artículo 2 numeral 3 de la Ley 81, el principio de lealtad señala que "los datos personales deberán recabarse sin engaño o falsedad y sin utilizar medios fraudulentos, desleales o ilícitos".

Este principio está directamente relacionado con la licitud y el consentimiento. Ya que, el responsable de tratamiento, en el momento de la recopilación, deberá obtener los datos personales solicitando a sus titulares su información de tal forma que, se garantice un consentimiento libre de vicios, de esta manera el tratamiento de datos personales será lícito.

viii. Proporcionalidad:

En cuanto al principio de proporcionalidad, el artículo 2 de la ley 81 determina que "solo deberán ser solicitados aquellos datos adecuados, pertinentes y limitados al mínimo necesario en relación con la finalidad para la que son requeridos".

En realidad, esta norma hace alusión a la minimización de datos, por la cual se limita el tratamiento al número de datos mínimo posible para llevar a cabo la finalidad establecida por el responsable. El estándar internacional establece a la proporcionalidad relacionada con los medios o mecanismos de tratamiento, de tal manera que no deban ser excesivos ni exorbitantes para el tratamiento de datos de un titular.

ix. Confidencialidad:

El numeral 7 del artículo 2 de la Ley 81 determina que el principio de confidencialidad establece que "todas las personas que intervengan en el tratamiento de datos personales están obligadas a guardar secreto o confidencialidad", impidiendo el acceso o uso no autorizado, incluso finalizada la relación con el titular o responsable del tratamiento de datos.

En este sentido, el artículo 9 de la citada Ley, precisa que la confidencialidad es obligatoria no solo para quienes tienen acceso a los datos personales sino incluso aquellas que estén involucradas en el tratamiento, tanto si son organismos públicos como privados. Quedan exentos de confidencialidad los datos que han sido recolectados de fuentes que no sean de dominio o acceso al público, así como sobre los demás datos y antecedentes relacionados con la base de datos, obligación que no cesa por haber terminado sus actividades en ese ámbito.

Se recalca que la Constitución Panameña concibe a la confidencialidad como derecho y no como principio, tal como se analizará en el acápite respectivo.

x. Licitud:

El numeral 8 del artículo 2 de la Ley 81 señala el principio de licitud por el cual para que el tratamiento de un dato personal sea lícito, los datos personales deben recolectarse: por disposición de la ley, ya sean estas normas especiales o los casos establecidos en el artículo 8 de la presente norma; o por autorización válida del titular, conforme se analizó en el principio de consentimiento, esto es libre de vicios, previamente informado e inequívoco.

i. Portabilidad:

La portabilidad aparece en la ley panameña concebida como principio y como derecho, a diferencia del modelo europeo que lo concibe únicamente como derecho.

El numeral 9 del artículo 2 de la Ley 81, que enlista los principios aplicables a la protección de datos personales, dispone que "el titular de los datos tiene derecho a obtener de parte del responsable del tratamiento una copia de los datos personales de manera estructurada en un formato genérico y de uso común".

De la redacción de esta norma consta que el principio es en realidad el reconocimiento de un derecho. De esta manera se intenta otorgar al titular del dato, la posibilidad de elegir el proveedor de acceso o de servicios que satisfaga sus necesidades, puesto que podrá solicitar la totalidad de su información para que ésta sea entregada al nuevo servicio y de esta forma se evite pérdida de información al producirse este cambio. De ahí la necesidad de que sea un formato portable, genérico que pueda ser utilizado por cualquier otro proveedor.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

El artículo 15 de la Ley 81 reconoce "como derechos irrenunciables básicos los derechos que tienen los titulares de datos personales, sin perjuicio de cualquier otro derecho reconocido en esta Ley". Es decir, los derechos de acceso, modificación, cancelación, oposición y portabilidad, pero además deja abierta la puerta a otros derechos que permitan la protección de la persona y sus datos.

Conforme señala el artículo 8 de la Ley 81, los titulares de los datos podrá ejercer sus derechos sin cargo alguno, en cualquier momento, los cuales son irrenunciables, sin perjuicio de lo que dispongan leyes especiales, incluso si las bases de datos son de aquellas creadas con anterioridad a la vigencia de la Ley, artículo 44 de la Ley 81.

Por lo tanto, el ejercicio de los citados derechos no puede ser limitado mediante ningún acto o convenio entre partes, cuyo caso se declarará nulo el acto de limitación, artículo 21 de la Ley 81. A menos que a través de estos derechos se intente impedir o entorpece el debido trámite dentro de un proceso administrativo o judicial o por seguridad del Estado, o aquellos dispuestos por ley, artículo 23 de la Ley 81.

a. Derecho de acceso

Tanto en la descripción del derecho a la protección de datos personales, contenido en el artículo 42 de la Constitución panameña, como en el artículo 44 relativo al *habeas data*, se menciona al derecho de toda persona a acceder a la información personal contenida en bases de datos o registros públicos y privados, con miras a garantizar el derecho de acceso a su información personal.

Asimismo, el numeral 1 del artículo 15 de la Ley 81 reconoce el derecho de acceso, como aquel que "permite al titular obtener sus datos personales que encuentren almacenados o sujetos a tratamiento en bases de datos de instituciones públicas o privadas, además de conocer el origen y la finalidad para los cuales han sido recabados".

Pero además, de conformidad con el artículo 16 de la citada ley, el acceso habilita al titular a disponer de la constancia de la base de datos actualizada.

En esta conceptualización del derecho de acceso se recalca su estrecha vinculación con la finalidad. Ahora bien, en otras legislaciones se lo relaciona también con el principio de transparencia o de información; ya que, los titulares tienen derecho a acceder a toda la información sobre ellos pero además, a las formas de tratamiento, finalidades, análisis

de riesgo e impacto, medidas de seguridad, identidad de los tratantes, es decir a todos las medidas o mecanismos que permiten al responsable el tratamiento de los datos personales.

Se aclara además, que este derecho de acceso permite al titular requerir información a cualquiera de los responsables de datos que suministran la información, cuando los datos personales se encuentran almacenados en una base de datos que se alimente de datos provistos por diversos organismos, artículo 22 de la citada Ley.

b. Derecho de rectificación

Tanto en la descripción del derecho a la protección de datos personales, contenido en el artículo 42 de la Constitución panameña, como en el artículo 44 relativo al *habeas data*, aparece de forma expresa el derecho de toda persona a requerir la rectificación y protección de sus datos personales en toda base de datos o registro público o privado. Adicionalmente, en la descripción de la acción de *habeas data* consta menciones a corregir, actualizar (no solo a rectificar).

En el mismo sentido, en el numeral 2 del artículo 15 de la Ley 81 señala que el derecho de rectificación "permite al titular solicitar la corrección de sus datos personales que sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes". En el mismo sentido, el artículo 17 de la cita Ley señala que los datos "deberán ser modificados cuando sean erróneos, inexactos, equívocos o incompletos…".

Para que opere este derecho es necesario que el dato carezca de veracidad y exactitud, por ello es que esta condición está atada a su actualidad. Es decir, se pueden modificar aquellos datos caducos, que son los que han perdido actualidad por que la ley lo ha dispuesto, por el cumplimiento de la condición o la expiración del plazo señalado para vigencia o, si no hubiera norma expresa, por el cambio de los hechos o circunstancia que consigna, artículo 4 de la Ley citada.

Ahora bien, la norma menciona también datos incorrectos o falsos, estos son aquellos que nunca gozaron de veracidad y que por lo tanto, no son desactualizados sino equivocados de origen ya sea por negligencia o dolo. También incluye los incompletos, que pueden ser actuales pero que por su falta de contenido resultan equívocos. Adicionalmente, menciona el término irrelevante que son datos que más bien pudieran ser susceptibles de eliminación en aplicación del derecho de oposición, pero que de la redacción de la norma panameña pareciera que deben ser modificados por otros relevantes.

Finalmente, otra de las cualificaciones que habilitan la corrección de los datos personales es su pertinencia, la que se comparará con la finalidad de su recogida y el consentimiento.

c. Derecho de oposición

El numeral 4 del artículo 15 de la Ley 81 reconoce el derecho de oposición por el cual "el titular, por motivos fundados y legítimos relacionados con una situación en

particular, puede negarse a proporcionar sus datos personales o a que sean objeto de determinado tratamiento, así como a renovar su consentimiento".

El derecho de oposición descrito en esta norma, contempla todos los supuestos comprendidos en los estándares internacionales, pues faculta al titular a la negativa de entregar sus datos, es decir la negativa del consentimiento o de su renovación; así como a la denegación de que sus datos puedan ser tratados de manera general o a través de un determinado mecanismo de tratamiento. Como vemos, el derecho de oposición se correlaciona directamente con el principio de consentimiento, así como con el de finalidad y proporcionalidad.

El legislador panameño no incluyó en este derecho a la revocatoria del consentimiento, aunque es posible realizarla en cualquier momento, solo que no admite efectos retroactivos, artículo 6 de la citada Ley.

d. Derecho de cancelación

En el derecho a la protección de datos personales, contenido en el artículo 42 de la Constitución panameña, así como en el artículo 44 relativo al *habeas data*, se distingue el derecho de toda persona a suprimir datos personales en toda base de datos o registros públicos o privados de conformidad con lo previsto en la ley.

El numeral 3 del artículo 15 de la Ley 81 determina el derecho de cancelación, con un contenido similar al de rectificación, pues permite al titular solicitar la "eliminación de sus datos personales incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes". Asimismo, el artículo 16 señala que el titular tendrá derecho a exigir que eliminen sus datos personales cuando "su almacenamiento carezca de fundamento legal, cuando no hayan sido expresamente autorizados o cuando estuvieren caducos".

Asimismo, en el artículo 4 se define a la eliminación o cancelación de datos como la acción de "suprimir o borrar de forma permanente los datos almacenados en base de datos, cualquiera que sea el procedimiento empleado para ello".

De lo transcrito, podemos concluir al igual que con el derecho de rectificación, que para ser eliminados los datos deben cumplir con cualquiera de las condicionantes establecidas en las normas citadas.

De las cuales, mencionamos nuevamente el término irrelevante que son datos en aplicación del derecho de oposición, pudieran ser eliminados, pero que la normativa panameña prefiere incluirlos en el derecho de cancelación para que el titular justifique la irrelevancia y por ende su eliminación.

En consecuencia se faculta la eliminación de los datos personales cuando exista ilicitud en el almacenamiento, por falta de ley, de autorización del titular, o de la caducidad de los datos. Respecto de los otros términos utilizados en la norma, se entiende que si cabe modificación, también eliminación cuando los datos no son de calidad por carecer de exactitud, veracidad y actualidad.

Si bien el artículo 4 de la norma, menciona el bloqueo de datos, esta posibilidad no consta descrita como parte del derecho de cancelación.

e. Del bloqueo de datos

Aunque no consta en la lista de derechos previstos en el artículo 15 de la Ley 81, aparecen varias referencias al bloqueo de datos en cada una de las normas generales que prescriben el ejercicio de los derechos de un titular.

Conforme señala el artículo 4 de la Ley 81, el bloqueo de datos es la restricción temporal de cualquier acceso o tratamiento de los datos almacenados.

El artículo 17 de la citada Ley señala que el responsable de una base de datos, respecto de los cuales no corresponda la cancelación, podrá bloquear los datos personales del acceso de terceros o para evitar su uso en otros fines que no hayan sido los expresamente autorizados, sin necesidad de requerimientos del titular, cuando existan pruebas de inexactitud, o esta no pueda ser establecida o están fuera de vigencia.

Conforme consta del texto, el bloqueo de datos no se concibe como derecho sino como obligación del responsable de tratamiento en aplicación del consentimiento, y de los principios de licitud y de veracidad y exactitud.

f. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

Este derecho se encuentra reconocido en el artículo 19 de la Ley 81 que determina que el titular de los datos personales tiene derecho "a no ser sujeto de una decisión basada únicamente en el tratamiento automatizado de sus datos personales, que produzca efectos jurídicos negativos o le produzca un detrimento a un derecho, cuyo objeto sea evaluar determinados aspectos de su personalidad, estado de salud, rendimiento laboral, crédito, fiabilidad, conducta, características o personalidad, entre otros".

Ahora bien, la citada norma establece los casos en los que es posible realizar valoraciones automatizadas, estos son: por consentimiento del titular; necesaria para celebrar o dar cumplimiento a un contrato o relación jurídica; autorizada por leyes especiales.

Este derecho, reconocido en la normativa europea ha sido incorporado en la legislación panameña debido a los avances tecnológicos que permiten realizar perfiles conductuales e incluso predictivos, y que pueden ser usados para el acceso o no a otros derechos fundamentales. La palabra únicamente no puede ser interpretada restrictivamente de tal manera que también es aplicable este derecho a los tratamientos semiautomatizados que realizan perfiles de personas. El titular tiene derecho entonces a que una decisión automatizada no le cause efectos negativos o detrimento de derechos, de tal manera que si esto ocurre pueda arbitrar los derechos de acceso, rectificación, eliminación y las indemnizaciones producto del perjuicio causado.

g. Derecho de consulta al registro general de protección de datos personales

El artículo 31 de la Ley 81 determina que los responsables llevarán un registro de la bases de datos que puedan cederse a terceros, las que deberán estar a disposición de la Autoridad Nacional de Transparencia y Acceso de la Información.

Los elementos que deberá contener el registro de cada una de las bases de datos son: la identificación de la base; el responsable; la naturaleza de los datos personales; el fundamento jurídico de su existencia; los procedimientos de obtención y tratamiento; el destino de los datos y las personas naturales o jurídicas a las que pueden ser transferidos; la descripción del universo de personas; las medidas de seguridad; los protocolos; la descripción técnica de la base de datos, forma y condiciones en las que las personas puedan recibir o acceder a los datos referidos a ellas; los procedimientos para que el titular ejerza sus derechos; el tiempo de conservación y cualquier cambio de los elementos indicados; así como, la identificación y periodo de todas las personas que han ingresado a los datos personales dentro de quince días hábiles desde que se inicie dicha actividad (art. 31).

De lo anterior, se destaca un tipo de registro que no suele constar descrito en las legislaciones de la región, esto es el registro del seguimiento que deben cumplir los responsables y que consiste en mantener la lista de las personas que han ingresado a los datos personales, pues este tracto sucesivo tiene como finalidad verificar la persona o personas que pudieran haber utilizado de forma inadecuada los datos personales.

Llama la atención el acápite final de la norma citada que señala que "solo pueden ser capturados para almacenamientos los datos obtenidos del documento de identidad personal que provea su titular". Esta excepción parece orientada a identificar la identidad de aquellas personas que pueden estar inmersas en estas bases de datos para efectos de verificación por parte de la autoridad de control. Sin embargo, por lo ambiguo de la redacción puede entenderse como otro de las formas de tratamiento dispuesta por ley sin necesidad de autorización del titular.

h. Derecho a indemnización por daños causados

El artículo 21 de la Ley 6 de 2002 determina que la persona afectada por haberse negado el acceso a la información, una vez cumplido con los requisitos y trámites expuestos en la presente ley, esto es la resolución favorable de una acción de *habeas data*, tendrá derecho a demandar civilmente al servidor público responsable por los daños y perjuicios que se le hayan ocasionado.

Por su parte, el artículo 37 de la Ley 81 determina que "el responsable del tratamiento de los datos personales deberá indemnizar el daño patrimonial y/o moral que causará por el tratamiento indebido de estos". En este caso, la normativa no establece el principio de responsabilidad, sin embargo incluye el claro reconocimiento de este tipo de indemnizaciones en el capítulo relativo a la responsabilidad por las infracciones cometidas. En suma, no es suficiente el acceso, la corrección o la eliminación del dato, sino que en aquellos casos en los que el inadecuado tratamiento ha causado daño, deberán ser indemnizadas a su titular.

Asimismo, el artículo 14 de la Ley 81 determina que esta responsabilidad civil sobre los daños o perjuicios causados se extiende al "custodio de la base de datos, por encargo o mandato del responsable del tratamiento de los datos personales, así como todo aquel que tenga acceso a los datos personales por razón de su relación a nivel jerárquico". Esta aclaración proviene no solamente de la solidaridad existente entre todos estos tratantes de datos sino a que, cada uno de ellos, debe demostrar que ha cumplido con diligencia las obligaciones asignadas por ley.

i. Derecho a la confidencialidad

En el artículo 44 de la Constitución panameña relativo al *habeas data* se determina que toda persona tiene derecho a que se mantenga en confidencialidad la información o datos que tengan carácter personal contenidos en bases de datos o registros públicos y privados. No obstante, el derecho de confidencialidad no es únicamente propio de la acción, sino sobre todo del contenido del derecho, aunque en el artículo 42 de la Constitución no se lo mencione.

La Ley 81 no concibe a la confidencialidad como derecho sino como principio, tal como se analizó en línea precedente.

De tal manera, la confidencialidad deberá mirarse en su doble virtualidad, derecho por su reconocimiento constitucional y principio conforme ley especializada. En consecuencia, podrá ser exigido por el titular como una prerrogativa propia, así como el responsable deberá aplicarlo de manera general en el tratamiento que realice y la autoridad velará por su efectivo cumplimiento desde los dos enfoques propuestos.

j. Derecho al olvido digital

No consta en la normativa constitucional ni legal panameña referencia a este derecho. Sin embargo, es menester señalar que este derecho era parte del Anteproyecto puesto en conocimiento de la Asamblea Nacional. En dicha versión se reconocía este derecho a personas naturales y jurídicas, no limitado solo a la desindexación, como ocurre en Europa, sino que se pretendía la eliminación en el origen, a través de los proveedores de servicios de hosting.

Ahora bien, debido al sonado caso Panamá Papers, por el cual el estudio jurídico Mossack Fonseca sufrió una filtración que desvelaba una lista de clientes titulares de compañías establecidas en Panamá, considerado paraíso fiscal para una gran parte de los países[1406]. Se consideró que estas personas de interés público no podían beneficiarse de la confidencialidad de sus datos debido a que por sus funciones o cargos manejaban recursos públicos y por lo tanto, al mantener sus recursos personales en este tipo de paraísos incumplían con leyes de sus países o incluso se encontraban cometiendo infracciones penales.

[1406] C. BOTERO CABRERA "Panamá Papers, entre transparencia y privacidad", El Espectador, accedido el 29 de agosto de 2019, https://www.elespectador.com/opinion/opinion/panama-papers-entre-transparencia-y-privacidad-columna-628488

De esta manera, la prensa logró que en la versión final de la normativa panameña no se incluya el derecho al olvido, por considerar que este podría afectar la libertad de información y que en la disputa entre intimidad y libertad de expresión, esta última prevalece en garantía de la transparencia y la democracia.

k. Spam

La Autoridad Nacional para la Innovación Gubernamental encabeza el CSIRT Panamá, quien mediante aviso 2014-07– Correos no deseados (spam) de 15 de abril de 2014, determina criterios que deben ser aplicados por usuarios del sistema de correo electrónico para evitar spam.[1407]

l. Derecho a la Portabilidad

Tal como señalamos en líneas precedentes, el artículo 2 numeral 9 de la Ley 81 señala a la portabilidad como principio, aunque lo define como derecho.

En el mismo sentido, el artículo 15 de la citada Ley señala que a través del derecho de portabilidad el titular tienen la facultad de "obtener una copia de los datos personales de manera estructurada, en un formato genérico y de uso común, que permita ser operado por distintos sistemas y/o transmitirlos a otro responsable". Pero a continuación establece una serie de condiciones que limitan el ejercicio de este derecho y que se refieren a que: el titular haya entregado sus datos directamente al responsable; se trate de un volumen relevante de datos, tratados de forma automatizada; el titular haya dado su consentimiento para el tratamiento; o, se requiera para ejecución o el cumplimiento de un contrato.

En suma, a la luz de la normativa panameña, la portabilidad deberá ser vista como derecho y principio que permite al titular disponer de sus datos para viabilizar un cambio entre proveedores de servicio, aunque las limitaciones impuestas en el artículo 15 de la citada norma son condiciones que atienden a la practicidad, porque no se podrá entregar datos que no se posea o que no estén automatizados, ya que podrían significar un esfuerzo desproporcionado para la entidad a la que se le solicita la portabilidad.

La causal que causa mayor confusión es aquella que menciona el consentimiento, por cuanto esto no impediría la entrega de la copia de la información sino que habilitaría la conservación de la data con fines contractuales o legales.

Tampoco es condición la transmisión efectiva de la información al otro operador, esto debido a que no se puede garantizar que el otro proveedor de servicio esté en capacidad de recibir la información, sino únicamente que este se encuentre en formato interoperable, esto es que permita ser operado por distintos sistemas.

m. Cesión

[1407] Autoridad Nacional para la Innovación Gubernamental, "CSIRT Panamá Aviso 2014-07– Correos no deseados (SPAM) – CSIRT Panamá", accedido 30 de diciembre de 2017, https://cert.pa/2014/04/csirt-panama-aviso-2014-07-correos-no-deseados-spam/.

Aunque no consta en la lista de principios descritos en el artículo 2 de la Ley 81, consideramos necesario analizar lo dispuesto en artículo 32 que determina que cuando un responsable tenga autorización legal o del titular para realizar transferencia de datos personales, mediante el uso de una red digital o de cualquier otro medio, excepto en los procesos internos del responsable del tratamiento de los datos, deberá dejarse constancia de: la individualización del requirente; el motivo y el propósito del requerimiento; los datos que se requiere que sean transferidos; la notificación a los titulares de los datos personales que integran el requerimiento, el motivo y el nuevo responsable de la información, salvo consentimiento previo por parte del titular; el tiempo máximo que el requirente utilizará los datos y la forma como serán destruidos una vez terminado su uso.

Todo ello, con la finalidad de salvaguardar los derechos de los titulares que deben conocer de las transferencias que se hayan realizado de sus datos, y permitir el trabajo de la Autoridad de control que a través de este registro puede realizar un adecuado trabajo de control.

En cuanto a la conservación de la data personal, el artículo 28 de la citada Ley, establece que:

> En ningún caso el responsable del tratamiento de datos personales y/o el custodio de la base de datos pueden transferir o comunicar los datos que relacionen con un persona identificada o identificable, después de transcurridos siete años desde que se extinguió la obligación legal de conservarla, salvo que el titular de los datos personales expresamente solicite lo contrario.

Esta norma además de mencionar que la transferencia puede realizarse tanto por el responsable como por el custodio de la información, determina el tiempo de conservación de la información, esto es 7 años, a menos que exista norma específica que habilite tiempo distinto. Tiempo suficiente para que el dato haya podido ser aprovechado por los tratantes de información.

g) *Procedimiento*

La acción constitucional aplicable es la de *habeas data* que es de carácter constitucional y desarrollado en ley específica: Ley 6 de 2002.

Ahora bien, la acción administrativa pertinente para el derecho de acceso está descrita en el artículo 16 de la Ley 81 que dispone:

> […] el titular de datos personales o quien lo represente podrá solicitar su información a los responsables del tratamiento de datos, la cual deberá ser proporcionada en un plazo no mayor de diez días hábiles, a partir de la fecha de presentación de dicha solicitud.

Es decir, será sujeto activo el titular o su representante legal. Mientras que sujeto pasivo será el responsable del tratamiento de datos. El ejercicio de estos derechos será gratuito y deberá realizarse en el plazo señalado en la ley.

De otro lado, el artículo 17 dispone el procedimiento administrativo pertinente para el ejercicio del derecho de rectificación o eliminación, que dispone que cuando los datos sean erróneos, inexactos, equívocos o incompletos el responsable tendrá un término de cinco días hábiles para satisfacer la solicitud.

Cuando el responsable de la base de datos personales no se pronuncia sobre las solicitudes realizadas por el titular de datos personales dentro de los términos establecidos, tendrá derecho a recurrir a la Autoridad Nacional de Transparencia y Acceso a la Información. Lo mismo si se trata de una entidad pública, pues el ciudadano deberá acudir a esta en primera instancia y en caso de falta de respuesta podrá recurrir a la Autoridad Nacional de Transparencia y Acceso a la Información, artículo 18 de la Ley 81.

Las decisiones de la Dirección competente para esta materia dentro de la Autoridad Nacional de Transparencia y Acceso a la Información serán impugnables mediante recurso de reconsideración ante esta Dirección y de Apelación que se interpondrá ante el director general de la Autoridad Nacional de Transparencia y Acceso a la Información como segunda instancia, los cuales se sustentarán en un término de cinco días, a partir del día siguiente hábil después de su notificación, artículo 36 de la Ley citada.

Finalmente, en el caso de que el inadecuado manejo de los datos personales haya causado perjuicio, se ha previsto que los tribunales de justicia conozcan de las demandas que se presenten contra los responsables del tratamiento de los datos personales con la finalidad de solicitar de ellos las indemnizaciones morales o patrimoniales por los daños y perjuicios causados, artículo 37 de la Ley citada.

h) Habeas data

a. Sujeto activo

Conforme señala el artículo 44 de la Constitución, que coincide con el artículo 17 de la Ley 6 que desarrolla la acción de *habeas data*, los titulares y legitimada para promover esta acción son todas las personas.

b. Sujetos pasivos u obligados

El artículo 44 de la Constitución señala, de manera indirecta e incluso confusa, que los sujetos pasivos de la acción de *habeas data* son los que recaban en bancos de datos o registros oficiales o particulares datos personales, cuando estos últimos traten de empresas que prestan un servicio al público o se dediquen a suministrar información. Por su parte, el artículo 17 de la Ley 6 de 2002 determina que será sujeto obligado el funcionario público titular o responsable del registro, archivo o banco de datos en el que se encuentra la información o dato personal reclamado, que no haya suministrado lo solicitado o, si suministrado lo requerido, se haya hecho de manera insuficiente o en forma inexacta. De este modo, estas dos normas se complementan para su funcionamiento en un ámbito estrictamente público.

c. Derechos tutelados por el habeas data

El artículo 44 de la Constitución establece como derechos tutelados por el *habeas data* al derecho de acceso a la información pública o de acceso libre, de conformidad con lo establecido en esta Constitución, así como también se podrá solicitar que se corrija, actualice, rectifique, suprima o se mantenga en confidencialidad la información o datos que tengan carácter personal. Se verifica, entonces, una naturaleza mixta puesto que el *habeas data* se considera, tanto para datos públicos como para datos personales, cuando en otras legislaciones se establece una acción constitucional propia denominada acceso a la información pública, y otra la de *habeas data* circunscrita exclusivamente a datos personales.

d. Procedencia del habeas data

Respecto de la procedencia, el artículo 44 de la Constitución únicamente realiza una vaga determinación relativa a que la procedencia de la acción constitucional se realizará de conformidad con lo establecido en la propia Constitución.

e. Procedimiento del habeas data

No consta en la norma constitucional panameña referencia el procedimiento de *habeas data*, sino que está descrita en la Ley 6 de 2002. En el artículo 18 de la ley en mención consta que el *habeas data* será de competencia de los Tribunales Superiores que conocen de la acción de amparo de garantías constitucionales, cuando el funcionario titular o responsable de registro, archivo o banco de datos, tenga mando y jurisdicción a nivel municipal o provincial. Cuando el titular o responsable del registro, archivo o banco de datos tenga mando y jurisdicción en dos o más provincias, o en toda la República, será de competencia del Pleno de la Corte Suprema de Justicia.

Asimismo, conforme reza en el artículo 19, la acción de *habeas data* se tramitará mediante procedimiento sumario sin formalidades y sin necesidad de abogado, de conformidad con las reglas de sustanciación, impedimentos, notificaciones y apelaciones, aplicables a la acción de amparo de garantías constitucionales.

i) Institucionalidad de protección

El artículo 34 de la Ley 81 crea el Consejo de Protección de Datos Personales como ente consultivo en la materia de protección de datos personales. Dicho Consejo estará conformado por: El ministro de Comercio e Industrias, quien la presidirá; el administrador general de la Autoridad de Portación al Consumidor y Defensa de la Competencia; El director general de Autoridad Nacional de Transparencia y Acceso a la Información, quien ejercerá la Secretaria de esta; El defensor del pueblo; un representante del Consejo Nacional de la Empresa Privada; un representante del Colegio Nacional de Abogados; un representante de la Asociación Bancaria de Panamá; un representante del Tribunal Electoral; un representante de la Cámara de Comercio, Industrias y Agricultura de Panamá. Durarán en sus funciones por un periodo de dos años.

Este ente consultivo tiene una conformación que refleja el ámbito de aplicación de la ley, esto es de amplia repercusión pues incluye varios sectores públicos y privados. La conformación de múltiples partes interesadas le permite tener una visión integral de protección y aplicación de la protección de datos personales.

Conforme el artículo 35, el citado Consejo de Protección de Datos Personales tendrá las facultades siguientes: asesorar a la Autoridad Nacional de Transparencia y Acceso a la Información, recomendar acciones, políticas públicas y reglamentos; evaluar casos que le sean presentados para consultar y brindar sus recomendaciones; desarrollar su reglamento interno.

Ahora bien, la autoridad competente que permite la aplicación de la Ley 81 es la Autoridad Nacional de Transparencia y Acceso a la Información, en adelante, ANTAI, que para el debido cumplimiento de sus funciones creará una Dirección dedicada a la ejecución de esta Ley, dentro de su estructura organizativa, para lo cual contará con los recursos presupuestarios y financieros necesarios, artículo 45 de la norma citada. Tomando en cuenta que empezará a regir a los dos años de su promulgación, artículo 47.

Para lo cual, el Orgánico Ejecutivo reglamentará la presente Ley en coordinación con Autoridad Nacional de Transparencia y Acceso a la Información, artículo 46.

No consta una norma que determine las competencias o atribuciones de la ANTAI, sino que estas se desprenden del análisis completo de la normativa. De tal manera que ANTAI o la Dirección creada para el efecto, será competente para:

- Resolver sobre el recurso presentado por el titular en el caso de que el responsable público o privado no se pronuncie sobre las solicitudes de acceso, rectificación, modificación o eliminación de datos personales dentro de los términos establecidos (art. 18);
- Solicitar información necesaria y efectuar verificaciones a fin de realizar las investigaciones administrativas relacionadas exclusivamente y en cada caso con la queja o denuncia presentada (art. 18).
- Determinar cuándo un dato es inexacto o cuándo carece de fundamento legal, sin perjuicio de lo dispuesto en leyes especiales que regulen materias específicas (art. 17);
- Sancionar a la "persona natural o jurídica responsable del tratamiento de los datos personales, así como al custodio de la base de datos, que por razón de la investigación de las quejas o denuncias que se les presenten y se les compruebe que han infringido los derechos del titular de los datos personales" (art. 36);
- Fijar los montos de las sanciones aplicables a las respectivas faltas, acordes a la gravedad de las faltas (art. 36); y,
- Reglamentar el procedimiento sancionatorio (art. 36).

Es cuestionable el establecimiento de la autoridad de control en Panamá. En primer lugar, no se menciona las condiciones mínimas de autonomía, independencia de sus decisiones, que incluso pueden afectar al propio estado.

Además, si bien existen otras legislaciones como la mexicana que determina que la misma autoridad que controla el acceso a la información pública será la encargada de los datos personales, sin embargo esta configuración no se limita a la creación de una dirección que dependa de esta entidad, sino un cambio en la concepción misma de la entidad que en adelante asume un rol adicional que debe compaginarse con el primigenio.

Adicionalmente, la forma dispersa del establecimiento de las competencias no permite visibilizar la fuerza coercitiva de una autoridad garante de la protección de los datos personales.

Finalmente, entre sus atribuciones hacen falta amplios mecanismos de investigación, que permitan prevenir inadecuados tratamientos, ya que solo están habilitados en los casos de queja, cuando debiera ser una atribución que pudiera realizarse de oficio y de manera indeterminada, se menciona la posibilidad de realizar inspecciones.

Tampoco constan atributos relacionados con la facultad de verificación del cumplimiento de la normativa, ni medidas de coerción como el apercibimiento que permitan a los responsables una adopción paulatina de la norma.

Podemos colegir entonces, que la autoridad de control de los datos personales en Panamá, a través de normativa de inferior nivel, deberá apuntalar su gestión para volverse realmente un ente garante y supervigilante del derecho.

j) Régimen sancionador

Conforme el artículo 20 de la Ley 6 de 2002 existe el capítulo VI, relativo las sanciones y responsabilidades personales de los funcionarios, cuyos artículos pertinentes determinan:

> Artículo 20. El funcionario requerido por el Tribunal que conoce del recurso de Hábeas Data, que incumpla con la obligación de suministrar la información incurrirá en desacato y será sancionado con multa mínima equivalente al doble del salario mensual que devenga.
>
> En caso de reincidencia, el funcionario será sancionado con la destitución del cargo.
>
> [...] Artículo 22**.** El funcionario que obstaculice el acceso a la información, destruya o altere un documento o registro, sin perjuicio de las responsabilidades administrativas y penales derivadas del hecho, será sancionado con multa equivalente a dos veces el salario mensual que devenga.
>
> Artículo 23. El monto de las multas impuestas por las sanciones establecidas en la presente Ley, será remitido a una cuenta especial para la Defensoría del Pueblo dentro de su presupuesto, y será destinado a programas de participación ciudadana.

De lo transcrito se determina que las sanciones se impondrán una vez que el funcionario se niegue a practicar la orden judicial que le obliga a entregar, modificar, actualizar, entre otros, los datos personales; esto es cuando procede la acción de *habeas data*. Las formas de sanciones son multas y en caso de reincidencia, la destitución del funcionario.

De otro lado, la normativa señala que se han categorizado varios tipos de infracciones que pueden suscitarse por el inadecuado manejo de datos personales: leves, graves o muy graves (art. 38).

Se considera infracción leve, "el no remitir y/o informar a la Autoridad Nacional de Transparencia y Acceso a la Información dentro de los plazos requeridos la información de lo ordenado en esta Ley, su reglamentación o cualquier otra disposición normativa" (art. 39).

En cambio serán infracciones graves: efectuar el tratamiento de datos personales sin haber obtenido el consentimiento de su titular, o haberlo obtenido sin respetar el procedimiento legal; infringir los principios y garantías; infringir el compromiso de confidencialidad; restringir o entorpecer la aplicación de los derechos de acceso, rectificación, cancelación y oposición; incumplir el deber de informar al titular afectado acerca del tratamiento de sus datos personales; almacenar o archivar datos personales sin contar con las adecuadas condiciones de seguridad; no atender la reiteración de requisitos u observaciones formalmente notificadas o no proporcionar la documentación o información formalmente; o entorpecer o no cooperar con la ANTAI (art. 40).

Se consideran infracciones muy graves: recopilar de datos personales en forma dolosa; no observar de las regulaciones establecidas respecto al tratamiento de los datos sensibles; no suspender el tratamiento de datos personales cuando existiera un previo requerimiento de la ANTAI; almacenar o transferir internacionalmente datos personales, violentando lo establecidos en esta Ley; reincidir en las faltas graves (art. 41).

De producirse el cometimiento de las infracciones referidas, serán aplicables, dependiendo de la gravedad de la infracción cometida (art. 36), las siguientes sanciones: citación ante la Autoridad Nacional de Transparencia y Acceso a la Información con relación a registros o atender faltas (falta leve); multas según su proporcionalidad (faltas graves); o, cláusula de los registros de la base de datos o suspensión e inhabilitación de la actividad de almacenamiento y / o tratamiento de datos personales de forma temporal o permanente, sin perjuicio de la multa correspondiente (faltas muy graves).

La ANTAI, fijará los montos de las sanciones aplicables a las respectivas faltas, acordes a su gravedad, que se establecerán desde mil balboas (B/.1000.00) hasta diez mil balboas (B/.10 000.00), así como reglamentará el procedimiento correspondiente. Las sanciones pecuniarias no hayan sido pagadas en el término concedido, se remitirán para su cobro a la Dirección General de Ingresos del ministerio de Economía y Finanzas (art. 36).

Para hacer cumplir la sanción de suspensión o clausura, la Autoridad Nacional de Transparencia y Acceso a la Información podrá requerir el auxilio de la Fuerza Pública (art. 43).

Los hechos que acarreen una sanción serán documentados de acuerdo con las formalidades legales y se realizarán informes estadísticos que permitan a la ANTAI establecer la gravedad, reiteración o reincidencia de la infracción cometida. Se considerará reincidencia cuando la misma falta se repita dentro de un periodo de tres años (art. 43).

De lo transcrito se puede colegir que, el régimen sancionatorio será el mecanismo con el cual la autoridad de protección podrá cumplir con su deber de control y vigilancia, pero que las multas y sanciones establecidas podrían no resultar suficientemente ejemplarizadoras para evitar que los responsables de tratamiento incurran en faltas. Hará falta, una entidad dedicada a vigilar el correcto comportamiento de los responsables y que arbitre sanciones para que efectivamente se logre un respeto a los datos personales.

k) Transferencia internacional de datos

Conforme el artículo 4 numeral 19 se entiende por transferencia de datos el:

> […] dar a conocer, divulgar, comunicar, intercambiar y/o transmitir, de cualquier forma y por cualquier medio, de un punto a otro, intra o extrafronterizo, los datos a personas naturales o jurídicas distintas del titular, ya sean determinadas o indeterminadas.

En este sentido, el artículo 33 de la Ley 81, señala que toda transferencia de datos personales, es lícita si se cumple al menos una de las condiciones siguientes: el titular haya otorgado su consentimiento; sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar; en cumplimiento de tratados internacionales ratificados por la República de Panamá; necesaria para la prevención o el diagnóstico médico, la prestación asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios; efectuada a cualquier sociedad del mismo grupo económico del responsable del tratamiento, siempre que los datos personales no sean utilizados para finalidades distintas las que originaron su recolección; para la salvaguarda de un interés público o para la representación legal del titular de los datos personales o administración de justicia; necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, o en casos de colaboración judicial internacional; necesaria para el mantenimiento o cumplimiento de una relación jurídica entre el responsable del tratamiento y el titular de los datos; requerida para concretar transferencias bancarias o bursátiles; cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, el lavado de activos, los delitos informáticos, la pornografía infantil y el narcotráfico; que tanto el responsable como el destinatario adopten mecanismos de autorregulación vinculante, siempre que estos sean acordes a las disposiciones previstas en esta Ley; que se realice en el marco de cláusulas contractuales que contengan mecanismos de protección de los datos personales acordes con las disposiciones previstas en la presente Ley, siempre que el titular sea parte.

En todos los casos, el responsable del tratamiento que transfiere los datos y el receptor de los datos personales serán responsables por la licitud del tratamiento de los datos transferidos.

Tal como está redactada la norma, la cesión de datos requiere las condiciones de licitud descritas, sin que se haga referencia a un régimen específico para datos transfronterizos.

De conformidad con lo transcrito, se concluye que el régimen de cesión de datos transfronterizos en Panamá se estructura desde la licitud del tratamiento, de tal manera que es posible tratar datos en los casos previstos en el artículo 33 de la Ley 81.

De esta forma se omite la gradación de niveles de protección propuesto en el modelo europeo. Ya que es suficiente incurrir en alguna de las causales previstas en la norma citada, dentro de la cual consta incluido precisamente el reconocimiento de niveles adecuados de protección, o de garantías suficientes a través de mecanismos de autorregulación; o de casos que por su importancia, su comunicación se encuentren autorizadas legalmente. Finalmente, no existe facultad asignada a la autoridad de control para que autorice una transferencia cuando esté por fuera de los casos estipulados en el citado artículo 33, como ocurre en otras normativas.

2.12 Honduras (2003)

La Constitución Política de Honduras de 1982 no incluía la figura constitucional del *habeas data*.[1408]

Es recién en el año 2003 por medio de las reformas introducidas mediante Decreto 243/2003 que se incluye en el título IV, denominado "De las garantías constitucionales", capítulo I, Habeas corpus, *habeas data* y el amparo, cuyo artículo 182 señala lo siguiente:

> Artículo 182.- El Estado reconoce la garantía de Hábeas Corpus o Exhibición Personal, y de Hábeas Data. En consecuencia en el Hábeas Corpus o Exhibición Personal, toda persona agraviada o cualquier otra en nombre de ésta tiene derecho a promoverla; y en el Hábeas Data únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados de la manera siguiente:
>
> [...] 2. El Hábeas Data: Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en caso de que fuere necesario, actualizarla, rectificarla y-o enmendarla.
>
> Las acciones de Hábeas Corpus y Hábeas Data se ejercerán sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles o inhábiles y libres de costas. Únicamente conocerá de la garantía del Hábeas Data la Sala de lo Constitucional de la Corte Suprema de Justicia, quien tendrá la obligación ineludible de proceder de inmediato para hacer cesar cualquier violación a los derechos del honor, intimidad personal o familiar y la propia imagen.
>
> [...] En ambos casos, los titulares de los órganos jurisdiccionales que dejaren de admitir estas acciones constitucionales, incurrirán en responsabilidad penal y administrativa.[1409]

Posteriormente, se efectuó otra reforma a la Constitución hondureña mediante Decreto 381-2005, 20 de enero del 2006, publicado en el Diario Oficial La Gaceta 30,920, 4 de febrero del 2006, que respecto del título IV, denominado "De las garantías constitucionales", capítulo I, "Habeas corpus, *habeas data* y el amparo" determina el nuevo contenido del artículo 182 de la siguiente manera:

[1408] Asamblea Nacional Constituyente, "Honduras: Constitución Política de 1982", *Political Database of the Americas*, 1982, accedido 5 de noviembre de 2017, http://pdba.georgetown.edu/Constitutions/Honduras/vigente.html.

[1409] Asamblea Nacional Constituyente, "Honduras: Constitución de 1982 modificada por Decreto 243/2003", accedido 5 de noviembre de 2017, http://pdba.georgetown.edu/Constitutions/Honduras/hond05.html.

> Artículo 182. El Estado reconoce la garantía de Hábeas Corpus o de exhibición Personal, y de Hábeas Data. En consecuencia en el Hábeas Corpus o exhibición Personal, toda persona agraviada o cualquiera otro en nombre de éste tiene derecho a promoverla; y en el Hábeas Data únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados de la manera siguiente:
>
> [...] EL HABÉAS DATA: Para obtener acceso a la información; impedir su transmisión o divulgación; rectificar datos inexactos o erróneos; actualizar información, exigir confidencialidad y la eliminación de información falsa; respecto de cualquier archivo o registro, privado o público, que conste en medios convencionales, electrónicos o informáticos, **que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen.** Esta garantía no afectará el secreto de las fuentes de información periodística.
>
> Las acciones de Hábeas Corpus o de Hábeas Data se ejercerán sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles e inhábiles y libres de costas. Únicamente conocerá de la garantía de Hábeas Data la Sala de lo Constitucional de la Corte Suprema de Justicia.
>
> Los titulares de los órganos jurisdiccionales no podrán desechar estas acciones constitucionales y tienen la obligación ineludible de proceder de inmediato para hacer cesar la violación a la libertad, la seguridad personal, el honor, la intimidad personal, familiar o la propia imagen.
>
> Los titulares de los órganos jurisdiccionales que dejaren de admitir estas acciones incurrirán en responsabilidad penal y administrativa.
>
> Las autoridades que ordenaren y los agentes que ejecutaren el ocultamiento del detenido o que en cualquier forma quebranten esta garantía incurrirán en el delito de detención ilegal[1410] (énfasis añadido).

Sobre este último texto se desarrollará el análisis del contenido esencial ya que no existe normativa de menor jerarquía ni especialidad que pueda guiar el análisis.

Si bien el Instituto de Acceso a la Información Pública, con el apoyo de la Agencia española de Cooperación Internacional para el Desarrollo (Aecid), elaboró en el año 2013[1411] el documento base para el Anteproyecto de Ley de Protección de Datos, sin embargo hasta la presente fecha sigue en trámite la elaboración de esta ley.

Cabe señalar además que la vigente norma constitucional hondureña señala en el artículo 76 los derechos al honor, a la intimidad personal, familiar y a la propia imagen.

[1410] Asamblea Nacional Constituyente, "Honduras: Constitución de 1982 modificada por Decreto 381/2005", *Political Database of the Americas*, 2006, accedido 5 de noviembre de 2017, http://pdba.georgetown.edu/Constitutions/Honduras/vigente.html.

[1411] Instituto de acceso a la información pública, "Anteproyecto de Ley de Protección de Datos Personales de la República de Honduras", accedido 5 de noviembre de 2017, http://cei.iaip.gob.hn/doc/Ley%20de%20Proteccion%20de%20Datos%20Personales.pdf.

a) Ámbito: Registros o ficheros públicos y privados

El artículo 182 de la Constitución de Honduras señala que el *habeas data* únicamente puede promoverla la persona cuyos datos personales o familiares consten en medios convencionales, electrónicos o informáticos, en cualquier archivo o registro, privado o público.

b) Naturaleza del dato

El mencionado artículo 182 señala que la garantía constitucional de *habeas data* protegerá datos personales o familiares que consten en los archivos, registros públicos o privados; que consten en medios convencionales, electrónicos o informáticos, que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen. Es una limitada concepción de la naturaleza del dato personal, pues no está asociado a un derecho autónomo, sino como consecuencia de la transgresión del derecho a la intimidad y a la propia imagen.

c) Sujeto activo

Conforme señala la norma constitucional hondureña, la garantía de *habeas data* únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados.

d) Sujeto pasivo

La norma constitucional, al señalar el ámbito de aplicación, también determina los sujetos pasivos de la garantía de *habeas data*, estos son los responsables de registros públicos o privados.

e) Objeto o bien jurídico

a. Derecho de información

No existe referencia a este derecho en la normativa hondureña.

b. Autodeterminación informativa

No existe referencia a este derecho en la normativa hondureña. Por el contrario, la garantía de *habeas data* expresamente señala que solo se protegerán datos que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen, lo que manifiesta la ausencia de un contenido propio, de un derecho autónomo basado en la autodeterminación informativa.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

No existe referencia a este derecho en la normativa hondureña.

d. Principios

i. Deber de información

No existe referencia a este derecho en la normativa hondureña.

ii. Pertinencia

No existe referencia a este derecho en la normativa hondureña.

iii. Calidad

No existe referencia a este derecho en la normativa hondureña.

iv. Finalidad

No existe referencia a este derecho en la normativa hondureña.

v. Seguridad

No existe referencia a este derecho en la normativa hondureña.

vi. Consentimiento

No existe referencia a este derecho en la normativa hondureña.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

a. Derecho de acceso

Únicamente se encuentra reconocido el derecho de acceso dentro de la garantía constitucional del *habeas data*, conforme el artículo 182 de la Constitución de Honduras.

En tal sentido, la norma establece que se activará esta garantía con la finalidad de obtener acceso a la información, es decir, datos personales o familiares respecto de cualquier archivo o registro, privado o público, que conste en medios convencionales, electrónicos o informáticos, que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen. Por la forma que consta redactada la norma, se entiende que el derecho de acceso constante en el *habeas data* se encuentra limitado por la condición dañosa que su recolección pueda significar.

b. Derecho de rectificación y actualización

Nuevamente el artículo 182 de la Constitución hondureña señala que el *habeas data* tiene la finalidad de rectificar datos inexactos o erróneos; actualizar información respecto de cualquier archivo o registro, privado o público, que conste en medios convencionales, electrónicos o informáticos, que produzca daño al honor, a la intimidad personal, familiar y a la propia imagen. Nuevamente, este derecho es limitado a la condición de producir un daño a los derechos fundamentales antes citados.

c. Derecho de oposición

No existe referencia a este derecho en la normativa hondureña.

d. Derecho de cancelación

El *habeas data* como garantía constitucional en Honduras permite exigir la eliminación de información falsa respecto de cualquier archivo o registro, privado o público, que conste en medios convencionales, electrónicos o informáticos, que produzca daño al honor, a la intimidad personal, familiar y a la propia imagen. La condición de falsedad también podría ser una limitación innecesaria en la norma puesto que existen otras condiciones por las cuales se justifica la cancelación del dato, esto es por ejemplo terminación de su utilidad o finalidad (art. 182, Constitución de Honduras).

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

No existe referencia a este derecho en la normativa hondureña.

f. Derecho de consulta al registro general de protección de datos personales

No existe referencia a este derecho en la normativa hondureña.

g. Derecho a indemnización por daños causados

No existe referencia a este derecho en la normativa hondureña.

h. Derecho a la confidencialidad

El *habeas data* contemplado en el artículo 182 señala que puede ser presentado para exigir confidencialidad de los datos personales almacenados en cualquier archivo o registro, privado o público, que conste en medios convencionales, electrónicos o informáticos, que produzca daño al honor, a la intimidad personal, familiar y a la propia imagen. Esta garantía no afectará el secreto de las fuentes de información periodística. En tal sentido, el derecho de confidencialidad se encuentra tutelado siempre y cuando por su intermedio se transgredan los derechos citados.

i. Derecho *al olvido digital*

No existe referencia a este derecho en la normativa hondureña.

j. Spam

No existe referencia a este derecho en la normativa hondureña.

k. Derecho de cesión

La norma constitucional expresamente señala que el *habeas data* también tiene como objetivo impedir la transmisión o divulgación de datos personales almacenados en registros públicos o privados, cualquiera sea el medio que lo contenga con tal de que se

produzca daño al honor, la intimidad y la propia imagen (art. 182, Constitución de Honduras).

g) Procedimiento

No existe procedimiento administrativo, debido a que no hay les especializada sobre la materia.

h) Habeas data

a. Sujeto activo

El sujeto activo del *habeas data*, de conformidad con el artículo 182 de la Constitución, es la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados, que conste en medios convencionales, electrónicos o informáticos, que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen.

La normativa, además, aclara que por tratarse de una garantía constitucional se ejercerán sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles e inhábiles y libres de costas. Esta desformalización pretende acercar esta garantía a la ciudadanía como mecanismo que pretende tutela judicial efectiva.

b. Sujetos pasivos u obligados

Como se señaló en líneas precedentes, al determinar el ámbito de aplicación del *habeas data* indirectamente se señala que son obligados los responsables de las bases de datos públicos o privadas donde se encuentren almacenados los datos personales.

c. Derechos tutelados por el habeas data

La norma constitucional en análisis expresamente señala que los derechos tutelados son el honor, la intimidad personal, familiar y la propia imagen toda vez que solo protegen datos personales que produzcan daño y que una vez activados los mecanismos jurisdiccionales expresamente se determina la obligación ineludible de proceder de inmediato para hacer cesar la violación a la libertad, la seguridad personal, el honor, la intimidad personal, familiar o la propia imagen. No concibe la autodeterminación informativa como elementos esenciales dentro del derecho a la protección de datos personales.

d. Procedencia habeas data

Conforme señala el artículo 182 de la Constitución hondureña, procede el *habeas data* para obtener acceso a la información; impedir su transmisión o divulgación; rectificar datos; actualizar información, exigir confidencialidad y su eliminación, pero señala expresamente que los datos deben ser inexactos o erróneos o la información falsa; así como que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen.

Existen varias condiciones para que opere el *habeas data*, y todas son concurrentes conforme consta de la redacción del citado artículo. En consecuencia, la norma, lejos de coadyuvar a la tutela de los datos personales, dificulta su aplicabilidad.

e. Procedimiento del habeas data

La norma constitucional hondureña determina que la única competente para conocer la garantía de *habeas data* es la Sala de lo Constitucional de la Corte Suprema de Justicia. Además, como forma de evitar dilaciones e ineficacia de la administración de justicia se determina que los titulares de los órganos jurisdiccionales no podrán desechar estas acciones constitucionales y tienen la obligación ineludible de proceder de inmediato para hacer cesar la violación a la libertad, la seguridad personal, el honor, la intimidad personal, familiar o la propia imagen. Además, precisa que los titulares de los órganos jurisdiccionales que dejaren de admitir estas acciones incurrirán en responsabilidad penal y administrativa.

i) Institucionalidad de protección

No existe referencia a este principio en la normativa general ni específica hondureña.

j) Régimen sancionador

No existe referencia a este principio en la normativa general ni específica hondureña, aunque la norma constitucional señala que los titulares de los órganos jurisdiccionales que dejaren de admitir estas acciones incurrirán en responsabilidad penal y administrativa. Esta referencia general permite determinar la existencia de un régimen sancionador que podría ser aplicable a los casos de procedibilidad descritos en el artículo 182 citado.

k) Transferencia internacional de datos

No existe referencia a este principio en la normativa general ni específica hondureña.

2.13 México (2007)

En México el derecho a la privacidad estaba reconocido desde la Constitución de 1917 con el texto siguiente:

> Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.[1412]

En cambio, la primera aproximación constitucional al derecho a la protección de datos personales aparece en las reformas a la Constitución de los Estados Unidos Mexicanos de 2007 (en adelante Constitución mexicana), la cual mediante el Decreto 7, 20 de julio

[1412] Congreso Constituyente de los Estos Unidos Mexicanos, "Constitución Política de los Estados Unidos Mexicanos, actualizada a 24 febrero de 2017", *LXIII legislatura - Cámara de Diputados del H. Congreso de la Unión*, 1917, accedido 20 de julio de 2017, http://www.diputados.gob.mx/LeyesBiblio/pdf/1_240217.pdf.

de 2007,[1413] modificó el título primero, el capítulo I denominado "De los Derechos Humanos y sus Garantías", de forma específica el artículo 6 referido al derecho a la información pública; allí se adicionaron dos fracciones, las números II y III, que establecen limitaciones al derecho de acceso de información pública:

> Artículo 6o. [...] A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> [...] II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
>
> III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos...[1414]

Es con la reforma de 2009, mediante Decreto 20, 1 de junio de 2009,[1415] que se reconoce de forma expresa y como derecho autónomo e independiente el derecho a la protección de datos personales al adicionarse el segundo párrafo del artículo 16 que textualmente dice:

> Artículo 16. [...] Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros...[1416]

Con la finalidad de visibilizar los continuos avances e inclusiones en el texto constitucional de los derechos de transparencia y protección de datos personales, se describen los artículos siguientes:

- Artículo 20 de la Constitución, por el cual se regula el proceso penal acusatorio y que respecto de los derechos de las personas imputadas señala el de restringirse la publicidad de una audiencia cuando se ponga en riesgo la revelación de datos legalmente protegidos (lit. B); y en cuanto a la víctima o al ofendido determina el derecho al resguardo de su identidad y otros datos personales en los siguientes casos: cuando sean menores de edad; cuando se trate de delitos de violación, trata de personas, secuestro o delincuencia organizada; y cuando a juicio del juzgador sea necesario para su protección,

[1413] Congreso General de los Estados Unidos Mexicanos, "Decreto No. 7 de 20/07/2007, por el que se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos", *Orden Jurídico Nacional*, 2007, accedido 20 de julio de 2017, http://www.ordenjuridico.gob.mx/Constitucion/reformas.php.

[1414] Congreso Constituyente de los Estos Unidos Mexicanos, "Constitución Política de los Estados Unidos Mexicanos, actualizada a 24 febrero de 2017", cit.

[1415] Congreso General de los Estados Unidos Mexicanos, "Decreto No. 20, de 01/06/2009, por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos", *Orden Jurídico Nacional*, 2009, accedido 20 de julio de 2017, http://www.ordenjuridico.gob.mx/Constitucion/reformas.php.

[1416] Congreso Constituyente de los Estos Unidos Mexicanos, "Constitución Política de los Estados Unidos Mexicanos, actualizado a 24 febrero de 2017".

salvaguardando en todo caso los derechos de la defensa. Párrafo reformado: DOF 14-07-2011.[1417]

- En la fracción XXIX-O del artículo 73, de la sección III, se señala que el Congreso tiene facultad para legislar en materia de protección de datos personales en posesión de particulares. Fracción adicionada: DOF 30-04-2009.[1418]
- En la fracción XXIX-S del artículo 73, sección III, se determina que el Congreso tiene facultad para expedir las leyes generales reglamentarias que desarrollen los principios y bases en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno. Fracción adicionada: DOF 07-02-2014.[1419]
- En la fracción II del artículo 105 consta que la Suprema Corte de Justicia de la Nación conocerá de las acciones de inconstitucionalidad, las cuales podrán ejercitarse por el organismo garante que establece el artículo 6° de esta Constitución en contra de leyes de carácter federal y local, así como de tratados internacionales celebrados por el Ejecutivo Federal y aprobados por el Senado de la República, que vulneren el derecho al acceso a la información pública y la protección de datos personales. Asimismo, los organismos garantes equivalentes en las entidades federativas, en contra de leyes expedidas por las Legislaturas locales, e inciso adicionado DOF 07-02-2014.[1420] Reformado: DOF 29-01-2016.[1421]

A partir de estas dos reformas constitucionales (2007 y 2009), se dictó en México la siguiente legislación de aplicación nacional, por la cual se divide en dos ámbitos generales el sistema de protección de datos personales, el primero los datos personales en poder del Estado y el segundo en manos de los particulares:

– Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, cuya fecha de publicación en el Diario Oficial de la Federación es el 11 de junio de 2002 y que fuera abrogada por la Ley Federal de

[1417] Congreso General de los Estados Unidos Mexicanos, "Decreto No. 27, de 14 de julio de 2011, por el que se reforman los artículos 19, 20 y 73 de la Constitución Política de los Estados Unidos Mexicanos", *Orden Jurídico Nacional*, 2011, accedido 21 de julio de 2017, http://www.ordenjuridico.gob.mx/Constitucion/reformas.php.

[1418] Congreso General de los Estados Unidos Mexicanos, "Decreto No. 18, de 30 de abril de 2009, por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos", *Orden Jurídico Nacional*, 2009, accedido 21 de julio de 2017, http://www.ordenjuridico.gob.mx/Constitucion/reformas.php.

[1419] Congreso General de los Estados Unidos Mexicanos, "Decreto No. 47, de 7 de febrero de 2014, por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia", *Orden Jurídico Nacional*, 2014, accedido 21 de julio de 2017, http://www.ordenjuridico.gob.mx/Constitucion/reformas.php.

[1420] Ibíd.

[1421] Congreso General de los Estados Unidos Mexicanos, "Decreto No. 59, de 29 de enero de 2016, por el que se declaran reformadas y derogadas diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de la reforma política de la Ciudad de México", *Orden Jurídico Nacional*, 2016, accedido 21 de julio de 2017, http://www.ordenjuridico.gob.mx/Constitucion/reformas.php.

Transparencia y Acceso a la Información Pública, 9 de mayo de 2015; su última modificación es del 27 de enero de 2017.[1422]

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares de 2010.[1423]
- Ley General de Transparencia y Acceso a la Información Pública, 4 de mayo de 2015.[1424]
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de 2017.[1425]

Existe también normativa de inferior nivel como el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, cuyas últimas reformas corresponden al 21 de diciembre de 2011.[1426]

De otro lado, el 28 de junio de 2018 México ratifica el Convenio Nº108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, adoptado en Estrasburgo, y el Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos adoptado en Estrasburgo, el 8 de noviembre de 2001. Dicha normativa entró en vigencia el 01 de octubre de 2018, de esta manera México es el segundo país latinoamericano en firmar este Convenio.

Para identificar el contenido esencial del derecho a la protección de datos personales en México acudiremos a la normativa constitucional citada y al contenido de las leyes nacionales mencionadas previamente. No se usará las leyes de cada estado que conforman la unión mexicana por cuanto son estas las que deben adaptar su normativa a las establecidas como de carácter nacional.

b) Ámbito: Registros o ficheros públicos y privados

La Ley Federal de Transparencia y Acceso a la Información Pública, modificada en 2017 (en adelante, LFTAIP), reformada en 2017, por su naturaleza, regula el orden público federal, esto es, garantiza el derecho de acceso a la Información Pública en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y

[1422] Congreso General de los Estados Unidos Mexicanos, "Ley Federal de Transparencia y Acceso a la Información Pública", *Cámara de Diputados del H. Congreso de la Unión estados mexicanos*, 2016, accedido 23 de julio de 2017, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf.

[1423] Congreso General de los Estados Unidos Mexicanos, "Ley Federal de Protección de Datos Personales en Posesión de los Particulares", 2010, accedido 23 de julio de 2017, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

[1424] Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, "Ley General de Transparencia y Acceso a la Información Pública", *Corpus iuris en materia de protección de datos personales / INAI /RIPD*, 2015, accedido 19 de julio de 2017, http://corpusiurispdp.inai.org.mx/iberoamericano/Instrumentos/LGTAIP.pdf.

[1425] Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, "Ley General de Protección de Datos Personales en posesión de sujetos obligados", *Corpus iuris en materia de protección de datos personales / INAI /RIPD*, 2017, accedido 19 de julio de 2017, http://corpusiurispdp.inai.org.mx/iberoamericano/Instrumentos/LGPDPPSO.pdf.

[1426] Presidencia de la República de los Estados Unidos Mexicanos, "Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares", accedido 24 de agosto de 2017, http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf.

fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos federales o realice actos de autoridad (art. 1). Mediante esta norma aparece en México las primeras menciones a la protección de datos personales y su sistema de protección en el sector público.

Por su parte, la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares de 2010,* LFPDPPP de 2010, señala como finalidad la protección de los datos personales en posesión de los particulares, con el propósito de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas (art. 1). De ese modo, mediante esta ley se regularán a los particulares, sean estas personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de: I. Las sociedades de información crediticia; y II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial (art. 2).

Respecto de la *Ley General de Transparencia y Acceso a la Información Pública de 2015*, LGTAIP de 2015, esta tiene como finalidad reglamentar el artículo 6o de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia y acceso a la información; y establecer principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las Entidades Federativas y los municipios (art. 1). Además, aparece como objetivo específico de este cuerpo legal el de regular la integración, organización y funcionamiento del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante un de conjunto orgánico y articulado de sus miembros, procedimientos, instrumentos y políticas (art. 28), así como establecer las bases de coordinación entre sus integrantes (art. 2, 27), establecer e implementar los criterios, lineamientos y a evaluar las acciones relativas a la política pública transversal de transparencia, acceso a la información y protección de datos personales (art. 28).

En otras de sus funciones primordiales, el Sistema Nacional tiene como funciones: III. Desarrollar y establecer programas comunes de alcance nacional, para la promoción, investigación, diagnóstico y difusión en materias de transparencia, acceso a la información, protección de datos personales y apertura gubernamental en el país (art. 31).

Finalmente, la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de 2017*, LGPDPPSO de 2017, desarrolla el contenido de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados. Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados. Se entiende por sujetos obligados aquellos que en virtud de esta ley, ya sea en el ámbito federal, estatal y municipal, por parte de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. Los sindicatos y

cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal sean responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares. En todos los demás supuestos diferentes a los mencionados en el párrafo anterior, las personas físicas y morales se sujetarán a lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (art. 1).

Además de regular a escala nacional, en los tres órdenes de gobierno el ejercicio pleno y respeto del derecho a la protección de datos personales y la difusión de una cultura de este derecho y su accesibilidad (art. 11), esta norma, a diferencia de la LPDP de 2010, detalla un amplio sistema de protección sobre todo relacionado con las acciones efectivas para el ejercicio del derecho a la protección de datos personales de tal forma que entre sus objetivos fundamentales constan:

> II. Establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos; III. Regular la organización y operación del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refieren esta Ley y la Ley General de Transparencia y Acceso a la Información Pública, en lo relativo a sus funciones para la protección de datos personales en posesión de sujetos obligados; IV. Garantizar la observancia de los principios de protección de datos personales previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia; [...] VI. Garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales; VII. Promover, fomentar y difundir una cultura de protección de datos personales; VIII. Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las disposiciones previstas en esta Ley, y IX. Regular los medios de impugnación y procedimientos para la interposición de acciones de inconstitucionalidad y controversias constitucionales por parte de los Organismos garantes locales y de la Federación; de conformidad con sus facultades respectivas (art. 2, LGPDPPSO).

Respecto de la interrelación de esta ley con la Ley General de Transparencia y Acceso a la Información Pública, el Sistema Nacional, acerca del derecho a la protección de datos personales:

> [...] tendrá como objetivo diseñar, ejecutar y evaluar un Programa Nacional de Protección de Datos Personales que defina la política pública y establezca, como mínimo, objetivos, estrategias, acciones y metas para: I. Promover la educación y una cultura de protección de datos personales entre la sociedad mexicana; II. Fomentar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición; III. Capacitar a los sujetos obligados en materia de protección de datos personales; IV. Impulsar la implementación y mantenimiento de un sistema de gestión de seguridad a que se refiere el artículo 34 de la presente Ley, así como promover la adopción de estándares nacionales e internacionales y buenas prácticas en la materia, y V. Prever los mecanismos que permitan medir, reportar y verificar las metas establecidas (art. 12, LGPDPPSO).

c) Naturaleza del dato personal

En el artículo 6º de la Constitución mexicana se menciona que la información que se refiere a la vida privada y los datos personales se tomará como principio o base para el ejercicio del derecho de acceso a la información; del mismo modo, dicho artículo determina que es parte de la naturaleza del dato su relación con un titular, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.[1427] De tal manera que se usa información y dato como sinónimos.

Mientras que en el artículo 16 de la Constitución mexicana, reformada en 2009, se reconoce expresamente el derecho a la protección de datos personales. En tal sentido, identifica como presupuesto de este derecho a los datos personales, señalando que será la ley la que determine en qué casos se establecerán excepciones a su tratamiento.[1428]

Por su parte la LFTAIP, reformada en 2017, señala como concepto central el de información pública que es aquella generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados en el ámbito federal y que por su finalidad es pública, accesible a cualquier persona y solo podrá ser clasificada excepcionalmente como reservada de forma temporal por razones de interés público y seguridad nacional o bien, como confidencial (art. 3). Es en esta última categoría que aparece una referencia en la citada Ley, por la cual se considera información confidencial aquella contiene datos personales concernientes a una persona física identificada o identificable (art. 113). Así, consta descrita en la legislación la naturaleza de los datos personales.

Respecto de la LFPDPPP de 2010, por ser la ley específica de la materia señala en el artículo 3, relativo al glosario de términos, que se entenderá por "Datos personales: Cualquier información concerniente a una persona física identificada o identificable".

La misma norma además señala que los datos personales sensibles serán aquellos que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. En particular, aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Por bases de datos, se entiende como el conjunto ordenado de datos personales referentes a una persona identificada o identificable. Y a la disociación como el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo, como mecanismo de seguridad para recopilar datos sin autorización del titular en los casos establecidos en la ley. Asimismo, se comprende por fuente de acceso público, aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación. Respecto de su tratamiento, se entenderá como la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales (art. 3).

[1427] Congreso Constituyente de los Estos Unidos Mexicanos, "Constitución Política de los Estados Unidos Mexicanos, actualizada a 24 febrero de 2017".
[1428] Ibíd.

Es necesario mencionar la afirmación de que los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos; este tipo de soporte también es reconocido en la normativa en virtud de que la forma de contención de los datos también debe ser un aspecto de necesaria regulación, en especial desde la perspectiva del titular de los datos (art. 22).

En suma, todos esos conceptos descritos coinciden con la conceptualización general que determina a los datos personales como aquellos vinculados a persona identificada e identificable y que además pueden estar contenidas en bases de datos, electrónicas o físicas, por la redacción general de la norma, que podrán ser disociadas y puestas en conocimiento mediante una fuente de acceso público, materia de protección precisamente por los posibles tratamientos a los que puede ser sometidos.

Por su parte, la LGTAIP de 2015 en el artículo 3 señala criterios aplicables a la información pública que por extensión, y en especial por ser parte del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, le son aplicables; estos son:

> Documento: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones y competencias de los sujetos obligados, sus Servidores Públicos e integrantes, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico;
>
> Expediente: Unidad documental constituida por uno o varios documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite de los sujetos obligados.

De esa manera, los datos personales podrán constar tanto en documentos como en expedientes; en otras palabras, se protege cualquier forma de organización de la información, en todas las formas posibles de soporte, incluidos el escrito, impreso, sonoro, visual, electrónico, informático u holográfico.

Respecto de conceptos como datos abiertos,[1429] formatos abiertos,[1430] formatos accesibles,[1431] información de interés público[1432] son criterios aplicables estrictamente a

[1429] "VI. Datos abiertos: Datos digitales de carácter público que son accesibles en línea que pueden ser usados, reutilizados y redistribuidos por cualquier interesado y que tienen las siguientes características:" accesibles, integrales, gratuitos, no discriminatorios, oportunos, permanentes, primarios, legibles por máquinas, en formatos abiertos, de libre uso. Congreso General de los Estados Unidos Mexicanos, "Ley Federal de Protección de Datos Personales en Posesión de los Particulares".

[1430] "X. Formatos Abiertos: Conjunto de características técnicas y de presentación de la información que corresponden a la estructura lógica usada para almacenar datos de forma integral y facilitan su procesamiento digital, cuyas especificaciones están disponibles públicamente y que permiten el acceso sin restricción de uso por parte de los usuarios". Ibíd.

[1431] "XI. Formatos Accesibles: Cualquier manera o forma alternativa que dé acceso a los solicitantes de información, en forma tan viable y cómoda como la de las personas sin discapacidad ni otras dificultades para acceder a cualquier texto impreso y/o cualquier otro formato convencional en el que la información pueda encontrarse". Ibíd.

[1432] "XII. Información de interés público: Se refiere a la información que resulta relevante o beneficiosa para la sociedad y no simplemente de interés individual, cuya divulgación resulta útil para que el público comprenda las actividades que llevan a cabo los sujetos obligados". Ibíd.

datos públicos debido a que los datos personales, por disposición expresa del artículo 3 de la LFTAIP, reformada en 2015, se los considera como confidenciales.

Finalmente, la LGPDPPSO de 2017, en el artículo 3 sobre conceptos aplicables a la ley, coincide con el concepto de datos personales recogido en la LFPDPPP de 2010: es cualquier información concerniente a una persona física identificada o identificable; determina además que debe considerarse que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente por medio de cualquier información.

Acerca de las bases de datos, además de determinar que son el conjunto ordenado de datos personales referentes a una persona física, identificada o identificable, admite que esta forma de organización está condicionada a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Sobre los datos personales sensibles, coincide plenamente con el concepto establecido en la LFPDPPP de 2010; solo aclara que los datos enunciados no son limitativos, sino enunciativos y que, por lo tanto, cabe calificarse como datos sensibles otros que cumplan con los criterios de afectar la esfera íntima, originar discriminación o un posible riesgo grave.

También determina conceptos casi idénticos para términos como tratamiento, disociación, fuentes de acceso público, y añade la denominada *evaluación de impacto* en la protección de datos personales, consistente en un:

> [...] documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoren los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable (art. 3).

Finalmente, y para que no quede duda de ello, el artículo 4 de la citada ley determina que será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

De esa manera, es evidente que tanto en la ley que regula el ámbito privado, como aquella que lo hace en el ámbito público, el concepto de dato personal coincide y se complementa señalando que es toda información sobre la persona identificada e identificable, y que se la protege independientemente del soporte en el cual esté contenido.

d) Sujeto activo

Se establece en el artículo 6o. de la Constitución mexicana de manera primaria a la protección de datos personales, determinando como titulares a "Toda persona sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a

la información pública, a sus datos personales o a la rectificación de éstos".[1433] Asimismo, en la reforma de 2009, el artículo 16, en la parte pertinente, vuelve a determinar como titulares de este derecho a toda persona.[1434] Se entiende, entonces, que desde la Constitución mexicana las personas naturales son titulares del derecho a la protección de datos personales, y por no constar mención expresa se excluye a los entes ficticios. Esta postura se materializa en la distinta normativa que en cada caso señala lo siguiente:

La LFTAIP, reformada en 2017, señala principalmente el derecho de acceso a la información pública, y en este contexto en el artículo 3 determina que toda persona podrá acceder a ella, y menciona que los particulares tendrán acceso a la misma en los términos que estas leyes señalan; esto se asimila al caso de los datos personales que por definición son confidenciales y que, sin embargo, sus titulares tienen derecho a acceder a ella.

La LFPDPPP de 2010 determina que se considerará como titular a la persona física a quien corresponden los datos personales; de esta manera cierra la posibilidad de que personas morales estén dentro del sistema de protección (art. 3). Asimismo, el capítulo III, denominado "De los derechos de los titulares de datos personales", establece que cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro (art. 22). En el mismo sentido, el capítulo IV, "Del ejercicio de los derechos de acceso, rectificación, cancelación y oposición", determina que el titular o su representante legal podrán solicitar al responsable en cualquier momento el acceso, rectificación, cancelación u oposición, respecto de los datos personales que le conciernen (art. 28), para ello es necesario que la petición contenga el nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud, los documentos que acrediten la identidad o, en su caso, la representación legal del titular, la descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y cualquier otro elemento o documento que facilite la localización de los datos personales (art. 29).

La LGTAIP de 2015 no realiza mención expresa sobre la titularidad del derecho a la protección de datos personales.

La LGPDPPSO de 2017, en el título primero, disposiciones generales, capítulo 1, "Del Objeto de la Ley", artículo 1, menciona nuevamente la frase genérica acerca de que toda persona como titular del derecho a la protección de sus datos personales..., y en el artículo 3 establece como titular a la persona física a quien corresponden los datos personales, dejando de lado de forma expresa a las personas morales.

e) Sujeto pasivo

No consta a nivel constitucional referencia a los sujetos obligados, sino únicamente una remisión general a la ley que regulará los aspectos no constantes en el texto

[1433] Congreso Constituyente de los Estos Unidos Mexicanos, "Constitución Política de los Estados Unidos Mexicanos, actualizada a 24 febrero de 2017".
[1434] Ibíd.

constitucional. En tal sentido, se hará referencia a lo que señalan las cuatro normas generales que desarrollan este derecho:

La LFTAIP, reformada en 2017, en cuyo capítulo II, "De los sujetos obligados" declara que son sujetos obligados a transparentar y permitir el acceso a la información y proteger los datos personales establecidos en las leyes de la materia y en la Ley General (art. 16) que obren en poder de los sujetos citados en el artículo 1. Siendo así, "cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos federales o realice actos de autoridad" (art. 9). Adicionalmente, los fideicomisos y fondos públicos, considerados entidades paraestatales por sí mismos, por intermedio de sus propias áreas, unidades de transparencia y comités de transparencia. En el caso de los fideicomisos y fondos públicos que no cuenten con estructura orgánica y, por lo tanto, no sean considerados una entidad paraestatal, así como de los mandatos públicos y demás contratos análogos, cumplirán con las obligaciones de esta ley mediante la unidad administrativa responsable de coordinar su operación (art. 14).

Respecto de las obligaciones, procedimientos y responsabilidades, esta norma señala en cuanto a protección de datos personales que los sujetos obligados deberán proteger y resguardar la información clasificada como reservada o confidencial (art. 11), y podrán ser acreedores de las sanciones y medidas de apremio establecidas en las mismas (art. 10).

LFPDPPP de 2010, la ley específica de la materia señala que serán sujetos obligados los particulares, sean personas físicas o morales de carácter privado, que lleven a cabo el tratamiento de datos personales, con excepción de: I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables; y II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial (art. 2).

Conforme el artículo 30, todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la presente ley. Asimismo, fomentará la protección de datos personales al interior de la organización.

Los sujetos obligados se clasifican en: encargado, persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable; responsable, persona física o moral de carácter privado que decide sobre el tratamiento de datos personales; y, tercero, la persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos (art. 3).

De acuerdo con el artículo 14, el responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta ley, debiendo adoptar las medidas necesarias para su aplicación, incluso cuando estos datos fueren tratados por un tercero a solicitud del responsable. Además, el responsable deberá tomar las medidas necesarias y suficientes para garantizar el aviso de privacidad y hacer que este se respete por parte de él y de terceros con los que guarde alguna relación jurídica.

Por su parte, la LGTAIP de 2015, en el artículo 3 señala criterios aplicables a la información pública que por extensión y en especial por ser parte del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales le son aplicables, estos son las áreas, entendidas como instancias que cuentan o puedan contar con la información y que, por ser parte del sector público, estén previstas en el reglamento interior, estatuto orgánico respectivo o equivalentes.

Ahora bien, en el capítulo III, "De los sujetos obligados", consta que son sujetos obligados a transparentar y permitir el acceso a su información y proteger los datos personales que obren en su poder: cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, considerados entidades paraestatales (art. 26), así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en los ámbitos federal, de las entidades federativas y municipales (art. 23).

Respecto de datos personales, exclusivamente estos sujetos deberán proteger y resguardar la información clasificada como reservada o confidencial; este es el caso de los datos personales.

La LGPDPPSO de 2017 determina que el ámbito de aplicación de esta norma es el público, de observancia general en toda la república pues protege los datos personales, en el ámbito federal, estatal y municipal, respecto de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. Los sindicatos y cualquier otra persona, física o moral, que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares. Quedan por fuera de la aplicación de esta ley, las personas físicas y morales que, en cambio, deberán sujetarse a lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (art. 1).

Para esa ley, como para las previamente analizadas, se entenderá por responsable a todo aquel sujeto obligado descrito en el citado artículo 1, ya que es el que decide sobre el tratamiento de datos personales; mientras que el encargado será la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable. Respecto de la actuación y responsabilidad del encargado, aclara que deberá realizar las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitar sus actuaciones a los términos fijados por el responsable (art. 58).

Con la finalidad de que opere esta limitación, la relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido (art. 59). Si el encargado incumple las instrucciones contenidas en el contrato y decide por sí mismo el tratamiento de los datos personales, asumirá el carácter de responsable (art. 60). El encargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos

personales por cuenta del responsable, siempre y cuando medie la autorización expresa de este último. El subcontratado asumirá el carácter de encargado (art. 61).

El responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la ley (art. 63).

Finalmente, mediante la obligación de los responsables de establecer mecanismos que permitan ejercer, en igualdad de circunstancias, su derecho tanto al acceso, a la información pública como a la protección de datos personales, se ha identificado un grupo de atención prioritaria como titulares de este derecho; estos son las personas con algún tipo de discapacidad o grupos vulnerabilidad (art. 86). En este sentido, los sujetos obligados promoverán acuerdos con instituciones públicas especializadas que pudieran auxiliarles a la recepción, trámite y entrega de las respuestas a solicitudes de información, en la lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente (art. 85).

f) Objeto o bien jurídico

a. Derecho de información

En la Constitución mexicana no aparece mención expresa al derecho a la información; sin embargo, en la ley aplicable consta lo siguiente:

La LFTAIP, reformada en 2017, hace alusión expresa al derecho de transparencia y acceso a la información pública, por lo que las referencias al derecho a la información son en este contexto y no relativas al derecho a la protección de datos personales. Por ejemplo, lo relativo a la denuncia que no versa sobre presuntos incumplimientos a las obligaciones de transparencia establecidas en la presente ley, o se refiere al ejercicio del derecho de información o al trámite del recurso de revisión, el Instituto dictará un acuerdo de desechamiento y, en su caso, dejará a salvo los derechos del promovente para que los haga valer por la vía y forma correspondientes (art. 89).

LFPDPPP de 2010, en México el derecho de información se materializa mediante el aviso de privacidad, ya que los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el Aviso de Privacidad al que está sujeto el tratamiento (art. 23).

Por eso, el responsable tiene la obligación de notificar a los titulares de los datos, la información que se recaba de ellos y con qué fines (art. 15). El aviso de privacidad contiene información básica relativa a la identidad y domicilio del responsable que los recaba; las finalidades del tratamiento de datos; las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos; los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta ley; en su caso, las transferencias de datos que se efectúen, y el procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad; en el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos (art.

16). Esta última referencia da cuenta que, a diferencia de otros países, es posible crear y tratar datos sensibles.

Cuando los datos personales se hayan obtenido personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, salvo información previa. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o mediante cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata quién es el responsable y la finalidad del tratamiento, y proveer de mecanismos para que el titular conozca el texto completo del aviso de privacidad. Los formatos mediante los cuales se ponen a disposición de los titulares los avisos de privacidad son: impresos, digitales, visuales, sonoros o cualquier otra tecnología (art. 17).

Cuando resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados en consideración al número de titulares, o a la antigüedad de los datos, previa autorización del Instituto, el responsable podrá instrumentar medidas compensatorias. El aviso de privacidad no es aplicable, cuando el tratamiento sea con fines históricos, estadísticos o científicos (art. 18).

La LGTAIP de 2015, respecto de los datos personales existentes en bases de datos públicas señala que los sujetos obligados serán responsables de poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el cual se establezcan los propósitos para su tratamiento, en términos de la normatividad aplicable, excepto en casos en que el tratamiento de los datos se realice en ejercicio de las atribuciones conferidas por ley (art. 68). Nuevamente, esta norma establece como mecanismo para efectivizar el derecho de información de las personas un documento que tiene las mismas finalidades que el aviso de privacidad descrito en la LFPDPPP de 2010.

Finalmente, la LGPDPPSO de 2017, coincidente con las leyes previamente analizadas, declara como mecanismo de implementación del derecho de información el aviso de privacidad, que por tratarse de personas públicas deberá ser difundido por los medios electrónicos y físicos con que cuente el responsable; deberá ser redactado y estructurado de manera clara y sencilla, cuya finalidad es que el titular pueda tomar decisiones informadas respecto de la existencia y características del tratamiento al que serán sometidos sus datos. Cabe señalar que solo para estos sujetos obligados es posible determinar que en caso de imposibilidad de dar a conocer al titular el aviso de privacidad de manera directa, o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emita el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (art. 26). Debe diferenciarse que para particulares las causales de esfuerzos desproporcionados son relativas al número de titulares de los datos o a la antigüedad de estos, mientras que para sujetos obligados por tratarse del ámbito público la calificación será realizada por la institucionalidad creada para el efecto, que además pondrá a disposición del titular el mentado aviso en dos modalidades: simplificado e integral. El aviso simplificado deberá estar siempre disponible para que el titular pueda manifestar su negativa al tratamiento de sus datos personales, para las finalidades o transferencias que requieran el consentimiento del titular, antes de que ocurra dicho tratamiento (art. 27).

b. Autodeterminación informativa

La Constitución mexicana señala, en el artículo 16, el derecho de toda persona al acceso, rectificación y cancelación, así como a manifestar la oposición de sus datos personales, excepto en los casos expresamente autorizados por la ley.[1435] En tal sentido, las facultades que les corresponden a los titulares para el ejercicio del objeto, en especial la de oponerse es una de las manifestaciones directas del derecho a la autodeterminación informativa, pues es su titular quien decide desde su propia visión qué información y en qué magnitud entrega y permite someter a tratamientos.

En el mismo sentido, la LFPDPPP de 2010, en las disposiciones generales establece que la mencionada ley es de orden público y de observancia general en toda la república, y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas (art. 1).

Las otras leyes analizadas no realizan referencia alguna a este contenido esencial del derecho, pero como hacen alusión directa a los derechos ARCO; estas se entienden como mecanismos eficaces que permiten su ejercicio.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

El artículo 16 de la Constitución mexicana delimita que será la ley la que establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, especialmente el relativo al consentimiento en la recogida y tratamiento. Estas excepciones se fundarán exclusivamente en razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.[1436]

La LFTAIP, reformada en 20*17*, establece como criterio general que para que los sujetos obligados puedan permitir el acceso a información confidencial requieren obtener el consentimiento de los particulares titulares de la información. En consecuencia, establece las excepciones en el artículo 117 de la citada ley, en el momento en que señala que no se requerirá el consentimiento del titular de la información confidencial cuando la información se encuentre en registros públicos o fuentes de acceso público; por ley tenga el carácter de pública; exista una orden judicial; por razones de seguridad nacional y salubridad general, o para proteger los derechos de terceros, se requiera su publicación, o cuando se transmita entre sujetos obligados y entre estos y los sujetos de derecho internacional, en términos de los tratados y los acuerdos interinstitucionales, siempre y cuando la información se utilice para el ejercicio de facultades propias de los mismos.

Así también, dicha norma establece un sistema que debe ser aplicado por el Instituto, denominado la prueba de interés público, que consiste en corroborar una conexión patente entre la información confidencial y un tema de interés público y la proporcionalidad entre la invasión a la intimidad ocasionada por la divulgación de la información confidencial y el interés público de la información.

[1435] Ibíd.
[1436] Ibíd.

Por su parte, la LFPDPPP de 2010 señala como norma general, que todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente ley (art. 8). Las salvedades constan descritas en el artículo 4 que determina que los principios y derechos previstos en esta ley, tendrán como límite respecto de su observancia y ejercicio: la protección de la seguridad nacional, el orden, seguridad y salud públicos, así como los derechos de terceros. Por eso, los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta ley y demás normatividad aplicable. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos. En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, acerca de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta ley (art. 7).

La LGTAIP de 2015 considera que la obtención y tratamiento de datos personales, en términos de lo que dispone esta ley, por parte de los sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto (art. 80). Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

El responsable podrá tratar datos personales para finalidades distintas a aquellas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la presente ley y demás disposiciones que resulten aplicables en la materia (art. 18). Este es un caso especial, pues la necesidad de mandato expreso de la ley para tratar datos personales es evidente, pero además las finalidades deben ser concretas, explícitas y legítimas, justificándose el caso de personas desaparecidas.

La LGPDPPSO de 2017 estipula que el derecho a la protección de los datos personales solo se limitará por razones de seguridad nacional, en términos de la ley en la materia, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

d. Principios

i. Deber de información

No existe referencia constitucional al respecto. La LFTAIP, reformada en 2017, como se enfatizó en líneas anteriores, regula especialmente el derecho de transparencia y acceso a la información pública, por lo que las referencias al derecho a la información son en este contexto y no relativas al derecho a la protección de datos personales.

La LFPDPPP de 2010 determina que los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la ley (art. 6). El principio de información se verifica cuando el responsable informa a los titulares de los datos, respecto a la información que se recaba de ellos y con qué fines, mediante el aviso de privacidad (art. 15).

Según la LGTAIP de 2015, los sujetos obligados serán responsables de los datos personales en su posesión y deberán por ello poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de la normatividad aplicable, excepto en casos en que el tratamiento de los datos se haga en ejercicio de las atribuciones conferidas por ley (art. 68); esto es la necesidad del aviso de privacidad para efectivizar el deber de información.

En la LGPDPPSO de 2017, al determinar los principios considera que el responsable deberá observar la licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales (art. 16). Coincide con lo señalado en la LFPDPPP de 2010, cuando determina que el responsable deberá informar a los titulares de los datos, sobre la información que se recaba de ellos y con qué fines, por medio del aviso de privacidad (art. 20).

ii. Pertinencia

No existe referencia constitucional. Respecto de la LFTAIP, reformada en 2017, su contenido sobre esta temática no alude al derecho a la protección de datos personales.

Respecto de la LFPDPPP de 2010, en el capítulo relativo a los "Principios de protección de datos personales" consta que los responsables en el tratamiento de datos personales deberán observar el principio de calidad, y en su concepto consta descrito, en parte, el principio de pertinencia (art. 6), puesto que el responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados. Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento (art. 11). De esta manera, el principio de licitud se incluye dentro del de pertinencia pues es parte condicionante de aquel.

Por su parte, la LGTAIP de 2015 establece que los sujetos obligados serán responsables de los datos personales en su posesión y, en relación con estos, deberán tratarlos solo cuando sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido, o dicho tratamiento se haga en ejercicio de las atribuciones conferidas por ley (art. 68).

En la LGPDPPSO de 2017 se establece que el responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de estos. Se presume

que se cumple con la calidad en los datos personales cuando estos son proporcionados directamente por el titular y hasta que este no manifieste y acredite lo contrario (art. 23).

iii. Calidad

No existe referencia constitucional. Respecto de calidad, la LFTAIP, reformada en 2017, no alude a este principio desde la perspectiva del derecho a la protección de datos personales, sino acerca del derecho de transparencia y acceso a la información pública.

La LGTAIP de 2015 determina que los sujetos obligados serán responsables de los datos personales en su posesión y procurarán que los datos personales sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido o dicho tratamiento se haga en ejercicio de las atribuciones conferidas por ley; que los datos personales sean exactos y actualizados; que se sustituyan, rectifiquen o completen, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación (art. 68).

Sobre la LFPDPPP de 2010, el responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados. Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento (art. 11). Dicha norma recoge todas las características necesarias para determinar que un dato cumple con el principio de calidad, e incluso integra en la misma norma el principio de pertinencia.

Por su parte, la LGPDPPSO de 2017 estipula que el responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de estos. Se presume que se cumple con la calidad en los datos personales cuando estos son proporcionados directamente por el titular y hasta que este no manifieste y acredite lo contrario (art. 23).

iv. Finalidad

No existe referencia constitucional sobre este principio. La LFTAIP, reformada en 2017, no hace referencia a este principio aplicado a la protección de datos personales.

La LFPDPPP de 2010 determina que el tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en el aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular (art. 12). El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el período de tratamiento de los mismos a efecto de que sea el mínimo indispensable (art. 13).

La LGTAIP de 2015 señala que los sujetos obligados serán responsables de los datos personales en su posesión, de comunicar a los titulares los propósitos para su tratamiento (art. 68).

Según la LGPDPPSO de 2017, todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera. El responsable podrá tratar datos personales para finalidades distintas a aquellas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la presente ley y demás disposiciones que resulten aplicables en la materia (art. 18).

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos. Los plazos de conservación de los datos personales no deberán exceder aquellos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento (art. 23).

v. Seguridad

No existe referencia de este principio en la Constitución. Entre tanto, la LFTAIP, reformada en 2017, alude a la seguridad, pero pese a que sus criterios pueden ser aplicables no hacen referencia expresa a datos personales.

La LFPDPPP de 2010 determina que todo responsable deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico (art. 19).

La LGTAIP de 2015 considera que los sujetos obligados serán responsables de los datos personales en su posesión y deberán adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado (art. 68).

La LGPDPPSO de 2017 determina que el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe.

Las medidas de seguridad adoptadas por el responsable deberán considerar: el riesgo inherente a los datos personales tratados; la sensibilidad de los datos personales tratados; y el desarrollo tecnológico, las posibles consecuencias de una vulneración para

los titulares; las transferencias de datos personales que se realicen; el número de titulares; las vulneraciones previas ocurridas en los sistemas de tratamiento, y el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión (art. 32).

Se describen, además, varias actividades interrelacionadas que deben ser realizadas por el responsable, así como documentadas y contenidas en un sistema de gestión, como por ejemplo las de crear políticas, definir funciones y obligaciones del personal a cargo, realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los mismos y los recursos involucrados en su tratamiento, como pueden ser de manera enunciativa más no limitativa, *hardware*, *software*, personal del responsable, entre otros (art. 33).

Para tal efecto, el responsable elaborará en el documento de seguridad: un instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas,[1437] físicas[1438] y administrativas[1439] adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee (art. 3). El responsable deberá actualizar el documento de seguridad cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo; derivado del monitoreo y revisión del sistema de gestión o para mitigar el impacto de una vulneración a la seguridad ocurrida. En el caso de producirse incidentes, estos deben ser reportados y controlados para garantizar protección posterior.

vi. Consentimiento

La LFTAIP, reformada en 2017, determina que para que los sujetos obligados puedan permitir el acceso a información confidencial, que en el caso de esta ley son los datos

[1437] "**Artículo 3.** [...] **XXIII. Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: **a)** Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; **b)** Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; **c)** Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y **d)** Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales". Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, "Ley General de Protección de Datos Personales en posesión de sujetos obligados", cit.

[1438] "**Artículo 3.** [...] **XXII. Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: **a)** Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; **b)** Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información; **c)** Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y **d)** Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad." Ibíd.

[1439] "**Artículo 3.** [...] **XXI. Medidas de seguridad administrativas:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales". Ibíd.

personales, se requiere el consentimiento de los particulares titulares de la información (art. 117).

La LFPDPPP de 2010 delimita al consentimiento como uno de los principios aplicables a la protección de datos personales (art.
6). Por eso, es que como norma general se establece que todo tratamiento de datos personales estará sujeto al consentimiento de su titular, entendido como la manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos (art. 3), salvo las excepciones previstas por la presente ley. Dicho consentimiento debe ser expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.

Como se analizó en su momento, el mecanismo para efectivizar la recogida del consentimiento es el aviso de privacidad, que es un documento físico, electrónico o en cualquier otro formato con el cual se verifica la aplicación del principio de información, pues permite al responsable poner a disposición del titular, antes del tratamiento de sus datos personales (art. 15), la existencia del archivo y los fines de la utilización de los mismos (art. 3).

Se deberá obtener consentimiento expreso del titular cuando se receptan datos financieros o patrimoniales, salvo las excepciones legales (art. 8). Asimismo, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, mediante su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca cuando se traten de datos personales sensibles.

No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado. Como se analizó previamente, esta posibilidad es posible incluso para sujetos particulares cuando en otras legislaciones es considerado delito recopilar datos sensibles.

Acerca de la LGTAIP de 2015, por tratarse de la Ley de Transparencia y Acceso a la Información Pública, cuando se refiere en ella la información confidencial en realidad se trata de datos personales; y para que los sujetos obligados puedan permitir el acceso a información confidencial requieren obtener el consentimiento de los particulares titulares de la información (art. 120). Es decir, nuevamente el consentimiento es el centro del sistema de protección; por este motivo los sujetos obligados serán responsables de los datos personales en su posesión y deberán poner a disposición de los titulares de los datos personales, un documento en el que se establezcan los propósitos para su tratamiento, denominado aviso de privacidad, con el cual se materializa el derecho y el deber de información y se efectúa una adecuada recolección de datos personales. Además, los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información de acuerdo con la normatividad aplicable, salvo autorización legal (art. 68).

En la LGPDPPSO de 2017, nuevamente el consentimiento es la regla general, como manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos (art. 3), que podrá manifestarse de forma expresa, cuando la voluntad del titular se exteriorice verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología; o tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, este no manifieste su voluntad en sentido contrario. Por regla general, será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente (art. 21). Este consentimiento, cuando se refiera a datos sensibles necesitará ser expreso de su titular, a menos que lo autorice la ley. En el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables. Para que proceda el consentimiento previo del titular para el tratamiento de los datos personales, este debe ser informado; esto es que el titular tenga conocimiento del aviso de privacidad antes del tratamiento a que serán sometidos sus datos personales (art. 20). Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, mediante su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de esta ley.

vii. Excepciones al consentimiento

La LFTAIP, reformada en 2017, determina que no se requerirá el consentimiento del titular de la información confidencial, que para los términos de esta ley son los datos personales, cuando: la información se encuentre en registros públicos o fuentes de acceso público; tenga por ley el carácter de pública; exista una orden judicial; por razones de seguridad nacional y salubridad general; o para proteger los derechos de terceros, se requiera su publicación; o se transmita entre sujetos obligados, y entre estos los sujetos de derecho internacional, en términos de los tratados y los acuerdos interinstitucionales. Además, el Instituto deberá aplicar la prueba de interés público, que consiste en corroborar una conexión patente entre la información confidencial y un tema de interés público, y la proporcionalidad entre la invasión a la intimidad ocasionada por la divulgación de la información confidencial y el interés público de la información (art. 117).

La LFPDPPP de 2010 establece que todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente ley (art. 8), las cuales son: cuando este expresamente previsto en una ley; los datos figuren en fuentes de acceso público; los datos personales se sometan a un procedimiento previo de disociación; tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes; sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o se dicte resolución de autoridad competente (art. 10).

Asimismo, las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando esté prevista en una ley o tratado en los que México sea parte; sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios; sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas; sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero; sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia; sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y sea necesaria para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular (art. 37).

La LGTAIP de 2015 señala que los sujetos obligados no requerirán el consentimiento del titular de la información confidencial cuando: la información se encuentre en registros públicos o fuentes de acceso público; por ley tenga el carácter de pública; exista una orden judicial; por razones de seguridad nacional y salubridad general, o para proteger los derechos de terceros se requiera su publicación, o cuando se transmita entre sujetos obligados, y entre estos los sujetos de derecho internacional, en términos de los tratados y los acuerdos interinstitucionales, siempre y cuando la información se utilice para el ejercicio de facultades propias de los mismos. Además, se menciona la prueba de interés público, por la cual se deberá corroborar una conexión patente entre la información confidencial y un tema de interés público y la proporcionalidad entre la invasión a la intimidad ocasionada por la divulgación de la información confidencial y el interés público de la información (art. 120).

Finalmente, la LGPDPPSO de 2017 determina que el responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos: cuando una ley así lo disponga; cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales; cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente; para el reconocimiento o defensa de derechos del titular ante autoridad competente; cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes; cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria; cuando los datos personales se sometan a un procedimiento previo de disociación, o cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia, o cuando los datos personales figuren en fuentes de acceso público (art. 22).

Se entenderá como fuentes de acceso público: las páginas de internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general; los directorios telefónicos en términos de la normativa específica; los diarios, gacetas o boletines oficiales, de acuerdo con su normativa; los medios de comunicación social, y los registros públicos conforme a las

disposiciones que les resulten aplicables. Para que los supuestos enumerados en el presente artículo sean considerados fuentes de acceso público, será necesaria que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contraprestación, derecho o tarifa. No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita (art. 5).

viii. Principio de responsabilidad

No aparece referencia ni en la Constitución ni en LFTAIP, reformada en 2017, ni en la LGTAIP de 2015. Entre tanto, la LFPDPPP de 2010 señala entre los principios aplicables el de responsabilidad (art. 6), por el cual, el responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta ley, debiendo adoptar las medidas necesarias para su aplicación, así como garantizar la ejecución del aviso de privacidad en el momento de la recogida y durante todo el tratamiento (art. 14).

La LGPDPPSO de 2017 señala el principio de responsabilidad, por el cual el responsable debe elaborar y revisar periódicamente políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable y asignar recursos para su ejecución, así como servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología; poner en práctica un programa de capacitación y actualización; establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales; establecer procedimientos para recibir y responder dudas y quejas de los titulares (art. 30).

ix. Principio de licitud

No existe referencia a este principio ni en la LFTAIP, reformada en 2017.

La LFPDPPP de 2010 señala entre los principios aplicables el de licitud (art. 6), por el cual los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta ley y demás normatividad aplicable. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos. En todo tratamiento de datos personales se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellas serán tratados según lo que acordaron las partes en los términos establecidos por esta ley (art. 7).

En la LGTAIP de 2015, aunque no menciona expresamente el principio de licitud si consta entre las obligaciones de los sujetos obligados la de tratar datos personales solo cuando estos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido o dicho tratamiento se haga en ejercicio de las atribuciones conferidas por ley.

La LGPDPPSO de 2017 determina que el responsable deberá observar el principio de licitud en el tratamiento de datos personales (art. 16). El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera (art. 17), para lo cual deberá estar justificado por

finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera (art. 18). Por eso, el responsable no deberá obtener y tratar datos personales a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad (art. 19).

g) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

La LFPDPPP de 2010 señala que todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la presente ley, entre los que constan los derechos ARCO. Asimismo, fomentará la protección de datos personales al interior de la organización (art. 30).

Únicamente, la LGPDPPSO de 2017 menciona entre sus definiciones la de Derechos ARCO, es decir, los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales (art. 3). Pero tanto la citada ley como la LFPDPPP de 2010 determinan capítulos completos relativos al Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición; en dichos textos constan el derecho que tiene todo titular o su representante legal para solicitar al responsable en cualquier momento el acceso, rectificación, cancelación u oposición, respecto de los datos personales que le conciernen (art. 28, LFPDPPP de 2010, y art. 43, LGPDPPSO de 2017).

a. Derecho de acceso

La Constitución mexicana, en el artículo 6, determina que toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de estos.[1440] De la misma manera, el artículo 16 menciona el derecho a la protección de datos personales cuando establece que toda persona tiene derecho al acceso, rectificación y cancelación de sus datos personales, así como a manifestar su oposición, en los términos que fije la ley. [1441]

En la LFTAIP, reformada en 2017, no consta referencia sobre este derecho.

La LFPDPPP de 2010 delimita que cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro (art. 22). Los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el aviso de privacidad al que está sujeto el tratamiento (art. 23).

La solicitud de acceso, rectificación, cancelación u oposición deberá contener lo siguiente: el nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud; los documentos que acrediten la identidad o, en su caso, la representación legal del titular, la descripción clara y precisa de los datos personales respecto de los

[1440] Congreso Constituyente de los Estos Unidos Mexicanos, "Constitución Política de los Estados Unidos Mexicanos, actualizada a 24 febrero de 2017".
[1441] Ibíd.

que se busca ejercer alguno de los derechos antes mencionados, y cualquier otro elemento o documento que facilite la localización de los datos personales (art. 29).

En la LGTAIP de 2015, los sujetos obligados serán responsables de los datos personales en su posesión y deberán adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso, rectificación, corrección y oposición al tratamiento de datos, en los casos que sea procedente, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con la normatividad aplicable (art. 68). En este caso, por tratarse de una norma de carácter público la forma en la que está abordado este derecho es desde la perspectiva de los sujetos obligados, puesto que deberán garantizar el ejercicio de este derecho.

La LGPDPPSO de 2017, en el capítulo específico titulado "De los derechos de acceso, rectificación, cancelación y oposición", determina que en todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen, de conformidad con lo establecido en el presente título. El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro (art. 43). En tal sentido y respecto del derecho de acceso, se determina que el titular tendrá derecho de acceder a sus datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento (art. 44).

b. Derecho de rectificación

La Constitución mexicana, en el artículo 16, menciona este derecho cuando se señala que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley.[1442]

En la LFTAIP, reformada en 2017, no consta referencia sobre este derecho.

La LFPDPPP de 2010 estipula que cualquier persona o su representante legal podrá ejercer los derechos de acceso, rectificación, cancelación y oposición (art. 22). El titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos (art. 24). Además de todos los requerimientos generales, en el caso de solicitudes de rectificación de datos personales, el titular deberá indicar las modificaciones a realizarse y aportar la documentación que sustente su petición (art. 31).

En la LGTAIP de 2015, al igual que como se vio para el derecho de acceso, la norma prevé la obligación de los sujetos públicos de adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso, rectificación, corrección y oposición al tratamiento de datos y de capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos (art. 68).

En la LGPDPPSO de 2017, al igual que en el caso del derecho de acceso, la normativa determina que en todo momento el titular o su representante podrán solicitar el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le

[1442] Ibíd.

conciernen (art. 43). En el caso del derecho rectificación, el titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados (art. 45); es decir, menciona la actualización como otro elemento adicional que no consta en la LFPDPPP de 2010 y que faculta la rectificación. Si bien pudiera estar contenido cuando se usa el término inexacto, sin embargo, su expresa mención evita cualquier tipo de interpretación y clarifica el tema.

c. Derecho de cancelación

La Constitución mexicana, en el artículo 16, declara que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación.[1443]

La LFTAIP, reformada en 2017, y la LGTAIP de 2015 no mencionan referencia al derecho de cancelación por tratarse de información pública.

La LFPDPPP de 2010 estipula que cualquier persona o su representante legal podrán ejercer los derechos de acceso, rectificación, cancelación y oposición (art. 22). El titular tendrá en todo momento el derecho a cancelar sus datos personales. La cancelación de datos personales dará lugar a un período de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El período de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento. Una vez cancelado el dato se dará aviso a su titular. Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también (art. 25). El artículo 3 señala en el glosario de términos, el relativo al bloqueo de los datos personales.

El responsable no estará obligado a cancelar los datos personales cuando: se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento; deban ser tratados por disposición legal; obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas; sean necesarios para proteger los intereses jurídicamente tutelados del titular; para realizar una acción en función del interés público; para cumplir con una obligación legalmente adquirida por el titular, y sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto (art. 26).

En la LGPDPPSO de 2017, el titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último (art. 46). Con relación a una solicitud de cancelación, el titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del responsable (art. 52).

[1443] Ibíd.

d. Derecho de oposición

La Constitución mexicana, en el artículo 16, menciona el derecho de toda persona a manifestar su oposición, en los términos que fije la ley.[1444]

La LFTAIP, reformada en 2017, y la LGTAIP de 2015 no mencionan referencia al derecho de oposición.

La LFPDPPP de 2010 menciona cuando define al consentimiento, que este podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos. Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello. De esta manera, se efectiviza en la práctica el derecho de oposición. Coincidente con esta aplicación del principio del consentimiento aparece expresamente regulado como derecho de oposición aquel por el cual el titular de los datos personales tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular (art. 27).

Según la LGPDPPSO de 2017, el titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese el mismo, cuando: aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, y sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento (art. 47). En el caso de la solicitud de oposición, el titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición (art. 52).

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

No existe referencia ni constitucional ni legal, excepto en la LGPDPPSO de 2017, respecto del derecho a no soportar valoraciones producto de procesos automatizados, por el cual el titular podrá oponerse al tratamiento de sus datos personales o exigir el cese del mismo, cuando sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento (art. 47). Este derecho está contenido dentro del de oposición y es tomado en la legislación mexicana como una manifestación del mismo.

[1444] Ibíd.

f. Derecho de consulta al registro general de protección de datos personales

No consta referencia ni constitucional ni legal

g. Derecho a indemnización por daños causados

No consta referencia sobre este tema en la Constitución mexicana ni en la LFTAIP, reformada en 2017, ni en LGTAIP de 2015.

La norma que regula particulares, esto es la LFPDPPP de 2010, señala que los titulares que consideren que han sufrido un daño o lesión en sus bienes o derechos como consecuencia del incumplimiento a lo dispuesto en la presente ley por el responsable o el encargado, podrán ejercer los derechos que estimen pertinentes para efectos de la indemnización que proceda, en términos de las disposiciones legales correspondientes (art. 58).

Las sanciones que se señalan en el procedimiento de sanciones se impondrán sin perjuicio de la responsabilidad civil o penal que resulte (art. 66).

La LGPDPPSO de 2017 declara que las responsabilidades que resulten de los procedimientos administrativos correspondientes son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos. Dichas responsabilidades se determinarán, en forma autónoma, mediante los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes; también se ejecutarán de manera independiente (art. 165).

Es decir, este derecho no consta expresamente señalado, sino que responde de forma directa al cumplimiento del principio de responsabilidad.

h. Derecho a la confidencialidad

No consta referencia sobre este tema en la Constitución mexicana.

La LFTAIP, reformada en 2017, determina que se considera como información confidencial la que contiene datos personales concernientes a una persona física identificada o identificable, además de otra como los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, entre otros, que no son parte de este análisis. La información confidencial no estará sujeta a temporalidad alguna y solo podrán tener acceso a ella los titulares de la misma, sus representantes y los servidores públicos facultados para ello (art. 113).

La única referencia que la LFPDPPP de 2010 presenta, es aquella por la cual señala que el responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de estos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable (art. 21). A diferencia de otras legislaciones, los datos sensibles no tienen el carácter de confidenciales, sino que pueden ser tratados previo el consentimiento expreso y por escrito del titular, y se podrán crear bases de datos que los contengan cuando se justifiquen con finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado (art. 9). Incluso los mecanismos como la

disociación de datos, que son las herramientas que utilizan otras legislaciones para tratar obligatoriamente datos sensibles, en la normativa mexicana no se usan sino que, de forma general, basta con que los datos personales se sometan a un procedimiento previo de disociación para que sea posible procesar datos personales, incluso aquellos catalogados como sensibles.

La LGTAIP de 2015 considera información confidencial la que contiene datos personales concernientes a una persona identificada o identificable, al igual que la LFTIP reformada en 2017, y conforme a aquella también admite que la información confidencial no estará sujeta a temporalidad alguna y solo podrán tener acceso a ella los titulares de la misma, sus representantes y los servidores públicos facultados para ello (art. 116).

La LGPDPPSO de 2017 estipula que, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener mecanismos y sistemas, así como medidas de seguridad de carácter administrativo, físico y técnico que garanticen su confidencialidad (art. 31) aplicables a todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, obligación que subsistirá aún después de finalizar sus relaciones con el mismo (art. 42). En la relación entre el responsable y el encargado se deberá guardar confidencialidad respecto de los datos personales tratados (art. 59).

i. Derecho al olvido digital

No consta referencia sobre este tema ni en la Constitución mexicana ni en la LFTAIP, reformada en 2017, ni en LGTAIP de 2015, ni en la LFPDPPP de 2010, ni en la LGPDPPSO de 2017.

Este es un tema inacabado de amplia discusión debido, principalmente, a los criterios vertidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), antes llamado Instituto Federal de Acceso a la Información como autoridad de protección de datos personales en el Caso de Carlos Sánchez Peña, quien es un empresario mexicano que solicitó a Google México que retirara varios resultados de búsqueda como el que titulaba "Fraude en Estrella Blanca alcanza a Vamos México". En el año 2014, el interesado intentó suprimir estos datos presentando su solicitud ante Google México, S de R.L. de C.V. Frente a su negativa, en enero de 2015 interpone acción ante el INAI, en expediente PPD.0094/14 Google México, S. de R.L. de C.V, 2015,[1445] el cual dispuso aplicar los derechos de oposición y cancelación a favor del interesado y, en consecuencia, ordenó el proceso sancionatorio contra Google México por no permitir el retiro de la información cancelada por el ciudadano. Además, determinó que Google México, S de R.L. de C.V. es el sujeto responsable que debió acoger la petición de oposición y cancelación, pues es el que efectúa el tratamiento de datos personales, toda vez que el buscador es parte de su objeto social, según su acta constitutiva, conforme con el numeral XIV del artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que

[1445] Instituto Federal de Acceso a la Información, IFAI, "Google México, S. de R.L. de C.V, expediente PPD.0094/14".

señala como responsable del tratamiento de datos a la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.[1446]

Posteriormente, la Red de Defensa de los Derechos Digitales presentó un amparo contra la resolución del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, representando a la Revista Fortuna, el cual fuera negado en primera instancia. Sin embargo, el recurso de revisión presentado ante el Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región concedió el amparo solicitado y anuló la orden de remover un enlace de una nota periodística sobre actos de corrupción, por cuanto consideró que existía una manifiesta violación al derecho de audiencia dentro del procedimiento PPD.0094/14, ya que "cuando el acto reclamado tiene como efecto el obstaculizar la disponibilidad de enlace en un motor de búsqueda, que disminuye y menoscaba de manera directa el derecho de las quejosas a difundir información en internet, lo que representa así una interferencia con su derecho de libertad de expresión, previsto en el artículo 6° constitucional.[1447] No obstante, el Tribunal determinó que no es "dable en esta vía de amparo el análisis del derecho de libertad de expresión, que como tercero interesado defiende la parte quejosa, porque en este momento los alcances del amparo se limitan a su derecho de audiencia para que en la instancia ordinaria el órgano especializado decida lo que en derecho proceda respecto de las pretensiones de las partes"[1448]. Todavía no existe resolución que determine los elementos y características que definan el derecho al olvido, por lo que el tema de fondo supervive.

j. Spam

No consta referencia sobre este tema ni en la Constitución mexicana ni en la LFTAIP, reformada en 2017, ni en LGTAIP de 2015, ni en la LFPDPPP de 2010; esto se debe a que este tema se aborda desde la perspectiva del derecho al consumidor o incluso se ha configurado un tipo penal al respecto. Para un análisis exhaustivo del tema, que incluye posibles reformas y un adecuado sistema de protección, se puede leer el artículo de Julio Téllez Valdés, titulado "Regulación del Spam en México"[1449].

h) Procedimiento

La LFTAIP, reformada en 2017, ni la LGTAIP de 2015 determinan procedimiento alguno para viabilizar los derechos ARCO.

Por su parte, la LFPDPPP de 2010 contiene dos tipos de procedimientos consecutivos para garantizar la vigencia de estos derechos.

[1446] Instituto Federal de Acceso a la Información, IFAI, "En un hecho sin precedente, el IFAI inició un procedimiento de imposición de sanciones en contra de Google México", 207d. C., accedido 23 de agosto de 2017, http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_noticias_IFAI_Ene-2015.pdf.

[1447] Naucalpan de Juárez, Estado de México, acuerdo del Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región, "Amparo de Revisión Revista Fortuna vs INAI, 74/2012", 2016, accedido 23 de agosto de 2017, http://sise.cjf.gob.mx/SVP/word1.aspx?arch=1100/110000001885932400010 01.docx_0&sec=_Mercedes__Santos_Gonz%C3%A1lez&svp=1.

[1448] Ibíd.

[1449] J. TÉLLEZ VALDÉS, "Regulación del Spam en México", accedido 23 de agosto de 2017, http://www.razonypalabra.org.mx/anteriores/n49/bienal/Mesa%205/JulioTellez.pdf.

i) Ejercicio de los derechos de acceso, rectificación, cancelación y oposición conforme la LFPDPPP de 2010

a. Sujeto activo

El titular o su representante legal podrán solicitar al responsable en cualquier momento los derechos ARCO (art. 28).

b. Sujeto pasivo

Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la presente ley. Asimismo, fomentará la protección de datos personales al interior de la organización (art. 30).

c. Derechos tutelados

Se protegerán los derechos ARCO; esto es acceso, rectificación, cancelación u oposición (art. 28).

d. Procedencia

El procedimiento es directo; es decir, la petición o solicitud deberá presentarse directamente a cada responsable de fichero o base de datos (art. 29).

e. Procedimiento

Se podrá iniciar mediante una solicitud que contendrá: el nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud; los documentos que acrediten la identidad o, en su caso, la representación legal del titular; la descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y cualquier otro elemento o documento que facilite la localización de los datos personales (art. 29). En el caso de solicitudes de rectificación de datos personales, el titular deberá indicar, además, las modificaciones a realizarse y aportar la documentación que sustente su petición (art. 31).

Posteriormente, el responsable en un plazo máximo de veinte días, contados desde la fecha en que se recibió la solicitud, comunicará al titular la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince días siguientes a la fecha en que se comunica la respuesta (art. 32).

La obligación de acceso a la información se dará por cumplida cuando se pongan a disposición del titular los datos personales; o bien, mediante la expedición de copias simples, documentos electrónicos o cualquier otro medio que determine el responsable en el aviso de privacidad. En el caso de que el titular solicite el acceso a los datos a una persona que presume es el responsable y esta resulta no serlo, bastará con que así se le indique al titular por cualquiera de los medios a que se refiere el párrafo anterior, para tener por cumplida la solicitud (art. 33).

El responsable podrá negarse cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello; cuando en su base de datos no se encuentren los datos personales del solicitante; se lesionen los derechos de un tercero; exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y cuando la rectificación, cancelación u oposición haya sido previamente realizada. La negativa podrá ser parcial en cuyo caso el responsable efectuará el acceso, rectificación, cancelación u oposición requerida por el titular. En todos los casos anteriores, el responsable deberá informar el motivo de su decisión y comunicarla al titular, o en su caso, al representante legal, en los plazos establecidos para tal efecto, por el mismo medio por el que se llevó a cabo la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes (art. 34).

La entrega de los datos personales será gratuita, debiendo cubrir el titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos. No obstante, si la misma persona reitera su solicitud en un período menor a doce meses, los costos no serán mayores a tres días de Salario Mínimo General Vigente en el Distrito Federal, a menos que existan modificaciones sustanciales al aviso de privacidad que motiven nuevas consultas (art. 35).

j) Del procedimiento de protección de derechos conforme la LFPDPPP de 2010

a. Sujeto activo

El procedimiento se iniciará a instancia del titular de los datos o de su representante legal (art. 45).

b. Sujeto pasivo

El responsable que no entregue al titular los datos personales solicitados, lo haga en un formato incomprensible, o se niegue a efectuar modificaciones o correcciones a los datos personales (art. 45).

c. Derechos tutelados

Se protegerán los derechos ARCO; esto es acceso, rectificación, cancelación u oposición (art. 45).

d. Procedencia

Este procedimiento es indirecto y de alzada ante la negativa o no contestación de la solicitud previa realizada directamente al responsable. Por eso, se iniciará ante el Instituto dentro de los quince días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable, o en el caso de que el titular de los datos no reciba respuesta cuando haya vencido el plazo de respuesta previsto para el responsable. La solicitud de protección de datos también procederá cuando el responsable no entregue al titular los datos personales solicitados, o lo haga en un formato incomprensible, se niegue a efectuar modificaciones o correcciones a los datos personales, o el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponda a la información requerida (art. 45). La protección

de datos será desechada por improcedente cuando: el Instituto no sea competente o haya conocido solicitud contra el mismo acto y resuelto respecto del mismo recurrente; se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el titular que pueda tener por efecto modificar o revocar el acto respectivo; se trate de una solicitud de protección de datos ofensiva o irracional, o sea extemporánea (art. 52).

e. Procedimiento

Recibida la solicitud de protección de datos, que por escrito libre o mediante los formatos del sistema electrónico que al efecto proporcione el Instituto con la información básica que ayude a su trámite (art. 46), el Instituto dará traslado de la misma al responsable, para que, en el plazo de quince días, emita respuesta, ofrezca las pruebas que estime pertinentes y manifieste por escrito lo que a su derecho convenga. El Instituto admitirá las pruebas que estime pertinentes o podrá solicitar las demás que estime necesarias. Concluido el desahogo de las pruebas, el Instituto notificará al responsable el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los cinco días siguientes a su notificación. En el plazo máximo de 50 días, que podrá ampliarse por una vez (art. 47), el Instituto resolverá una vez analizadas las pruebas y demás elementos de convicción incluidos aquellos que deriven de la o las audiencias que se celebren con las partes (art.45).

En el caso de que la resolución de protección de derechos resulte favorable al titular de los datos, se requerirá al responsable para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de protección, debiendo dar cuenta por escrito de dicho cumplimiento al Instituto dentro de los siguientes diez días (art.48).

Las resoluciones del Instituto podrán: I. Sobreseer o desechar la solicitud de protección de datos por improcedente, o II. Confirmar, revocar o modificar la respuesta del responsable (art. 51).

La solicitud de protección de datos será sobreseída cuando: el titular fallezca; el titular se desista de manera expresa; sobrevenga una causal de improcedencia, y por cualquier motivo quede sin materia la misma (art. 53).

El Instituto podrá, en cualquier momento del procedimiento, buscar una conciliación entre el titular de los datos y el responsable. De llegarse a un acuerdo de conciliación entre ambos, este se hará constar por escrito y tendrá efectos vinculantes (art. 54).

Contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa (art.56).

El Instituto verificará el cumplimiento de la presente ley y de la normatividad que de esta derive. La verificación podrá iniciarse de oficio o a petición de parte. La verificación de oficio procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos o se presuma fundada y motivadamente la existencia de violaciones a la presente ley (art. 59).

Si con motivo del desahogo del procedimiento de protección de derechos o del procedimiento de verificación que realice el Instituto, este tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de esta ley, iniciará el procedimiento a que se refiere este capítulo, a efecto de determinar la sanción que corresponda (art. 61).

Contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa (art. 56).

Por su parte, LGPDPPSO de 2017 estipula dos tipos de procedimientos consecutivos para garantizar la vigencia de estos derechos.

k) Del ejercicio de los derechos de acceso, rectificación, cancelación y oposición conforme la LGPDPPSO de 2017

a. Sujeto activo

Los titulares para el ejercicio de los derechos ARCO deberán acreditar su identidad o la de personalidad con la que actúe el representante. Menores de edad o personas que se encuentren en estado de interdicción o incapacidad estarán sujetas a las reglas de representación generales. Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere el presente capítulo, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto (art. 49).

b. Sujeto pasivo

Los sujetos obligados, descritos en el artículo 1 de la citada ley, son cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal.

Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del responsable, que el titular considere competente (art. 52).

c. Derechos tutelados

Conforme el nombre del capítulo de la ley en análisis, los derechos tutelados son los de acceso, rectificación, cancelación y oposición.

d. Procedencia

Procede cuando a criterio de un titular se requiera el acceso, la rectificación, la cancelación y la oposición.

De esa manara, las únicas causas en las que el ejercicio de los derechos ARCO no será procedente son: cuando el titular o su representante no estén debidamente acreditados para ello; los datos personales no se encuentren en posesión del responsable; exista un

impedimento legal; se lesionen los derechos de un tercero; se obstaculicen actuaciones judiciales o administrativas; exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos; cuando la cancelación u oposición haya sido previamente realizada; el responsable no sea competente; cuando sean necesarios para proteger intereses jurídicamente tutelados del titular; sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular; cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano, o cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a este, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades (art. 55).

e. Procedimiento

Se interpondrá petición mediante escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto establezca el Instituto y los organismos garantes, en el ámbito de sus respectivas competencias (art. 52). El ejercicio de los derechos ARCO deberá ser gratuito. Solo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, excepto cuando el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir datos personales (art. 50).

El responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO, cuyo plazo de respuesta no deberá exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud. El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al titular dentro del plazo de respuesta.

En caso de resultar procedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días, contados a partir del día siguiente en que se haya notificado la respuesta al titular (art. 51).

La solicitud de acceso contendrá: el nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones; los documentos que acrediten la identidad del titular o de su representante; de ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud; la descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO; la descripción del derecho ARCO que se pretende ejercer, esto es las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del responsable en el caso de la cancelación, las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición; lo que solicita el titular, y cualquier otro elemento o documento que facilite la localización de los datos personales (art. 52).

Cuando el responsable no sea competente para atender la solicitud para el ejercicio de los derechos ARCO, deberá hacer del conocimiento del titular dicha situación dentro de los tres días siguientes a la presentación de la solicitud, y en caso de poderlo determinar, orientarlo hacia el responsable competente.

En caso de que el responsable exponga la inexistencia de los datos personales en sus archivos, registros, sistemas o expediente, dicha declaración deberá constar en una resolución del Comité de Transparencia que confirme la inexistencia de los datos personales.

l) Recurso de revisión

a. Sujeto activo

Será sujeto activo el titular o su representante (art. 94), quien podrá acreditar su identidad mediante identificación oficial, firma electrónica avanzada o del instrumento electrónico que lo sustituya, o mecanismos de autenticación autorizados por el Instituto y los organismos garantes (art. 95).

Cuando el titular actúe mediante un representante, este acreditará su personalidad, si se trata de una persona física, por medio de carta poder simple suscrita ante dos testigos, anexando copia de las identificaciones de los suscriptores, o instrumento público, o declaración en comparecencia personal del titular y del representante ante el Instituto o si se trata de una persona moral, mediante instrumento público (art. 96).

Respecto de datos de personas fallecidas, podrá interponer el recurso la persona que acredite tener un interés jurídico o legítimo (art. 97).

b. Sujeto pasivo

El Instituto o los organismos garantes (art. 94).

c. Derechos tutelados

Se protegerán los derechos ARCO; esto es acceso, rectificación, cancelación u oposición.

d. Procedencia

Contra la negativa de dar trámite a toda solicitud para el ejercicio de los derechos ARCO, o por falta de respuesta del responsable, procederá la interposición del recurso de revisión a que se refiere el artículo 94 de la presente ley (art. 56). De este modo, es un recurso de alzada que pretende conminar al responsable que no ha dado respuesta o esta no ha sido favorable al peticionario.

El recurso de revisión procederá cuando: se clasifiquen como confidenciales los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables; se declare la inexistencia de los datos personales; se declare la incompetencia por el responsable; se entreguen datos personales incompletos; se entreguen datos personales que no correspondan con lo solicitado; se niegue el acceso,

rectificación, cancelación u oposición de datos personales; no se dé respuesta a una solicitud para el ejercicio de los derechos ARCO dentro de los plazos establecidos; se entregue o ponga a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible; el titular se inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales; se obstaculice el ejercicio de los derechos ARCO, a pesar de que fue notificada la procedencia de los mismos; no se dé trámite a una solicitud para el ejercicio de los derechos ARCO, y en los demás casos que dispongan las leyes (art. 104).

El recurso de revisión podrá ser desechado por improcedente cuando: sea extemporáneo; el titular o su representante no acrediten debidamente su identidad y personalidad de este último; el Instituto o, en su caso, los organismos garantes hayan resuelto anteriormente en definitiva sobre la materia del mismo; no se actualice alguna de las causales del recurso de revisión previstas en el artículo 104 de la presente ley; se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el recurrente, o en su caso, por el tercero interesado, en contra del acto recurrido ante el Instituto o los organismos garantes; el recurrente modifique o amplíe su petición en el recurso de revisión, únicamente respecto de los nuevos contenidos, o el recurrente no acredite interés jurídico. El desecho no implica la preclusión del derecho del titular para interponer un nuevo recurso de revisión (art. 112).

e. Procedimiento

El recurso podrá interponerse por escrito libre en el domicilio del Instituto o los organismos garantes, o en las oficinas habilitadas; por correo certificado con acuse de recibo, por formatos, medios electrónicos, o cualquier otro medio que al efecto establezca el Instituto o los organismos garantes (art. 94).

El escrito de interposición del recurso de revisión contendrá: el área responsable ante la cual se presentó la solicitud para el ejercicio de los derechos ARCO; el nombre del titular que recurre o su representante y, en su caso, del tercero interesado, así como el domicilio o medio que señale para recibir notificaciones; la fecha en que fue notificada la respuesta al titular, o bien, en caso de falta de respuesta la fecha de la presentación de la solicitud para el ejercicio de los derechos ARCO; el acto que se recurre y los puntos petitorios, así como las razones o motivos de inconformidad; en su caso, copia de la respuesta que se impugna y de la notificación correspondiente, y los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante. Al recurso de revisión se podrán acompañar las pruebas y demás elementos que considere el titular procedentes someter a juicio del Instituto o, en su caso, de los organismos garantes (art. 105).

Una vez admitido el recurso de revisión, el Instituto o, en su caso, los organismos garantes podrán buscar una conciliación entre el titular y el responsable. De llegar a un acuerdo, este se hará constar por escrito y tendrá efectos vinculantes. El recurso de revisión quedará sin materia y el Instituto o, en su caso, los organismos garantes, deberán verificar el cumplimiento del acuerdo respectivo (art. 106).

El Instituto y los organismos garantes resolverán el recurso de revisión en un plazo que no podrá exceder de cuarenta días, el cual podrá ampliarse hasta por veinte días una sola vez (art. 108).

Las resoluciones del Instituto o de los organismos garantes podrán: sobreseer o desechar el recurso de revisión por improcedente; confirmar la respuesta del responsable; revocar o modificar la respuesta del responsable, u ordenar la entrega de los datos personales, en caso de omisión del responsable. Las resoluciones establecerán los plazos y términos para su cumplimiento y los procedimientos para asegurar su ejecución. Los responsables deberán informar al Instituto o a los organismos garantes el cumplimiento de sus resoluciones. Ante la falta de resolución por parte del Instituto o de los organismos garantes, se entenderá confirmada la respuesta del responsable. Cuando el Instituto o los organismos garantes determinen durante la sustanciación del recurso de revisión que se pudo haber incurrido en una probable responsabilidad por el incumplimiento a las obligaciones previstas en la presente ley y demás disposiciones que resulten aplicables en la materia, deberán hacerlo del conocimiento del órgano interno de control o de la instancia competente para que esta inicie, en su caso, el procedimiento de responsabilidad respectivo (art. 111).

El recurso de revisión solo podrá ser sobreseído cuando: el recurrente se desista expresamente; el recurrente fallezca; admitido el recurso de revisión, se actualice alguna causal de improcedencia en los términos de la presente ley; el responsable modifique o revoque su respuesta de tal manera que el recurso de revisión quede sin materia (art. 113).

El Instituto y los organismos garantes deberán notificar a las partes y publicar las resoluciones, en versión pública, a más tardar, al tercer día siguiente de su aprobación (art. 114).

m) Recurso de inconformidad

a. Sujeto activo

El titular o su representante (art. 94).

b. Sujeto pasivo

El Instituto o los organismos garantes podrán interponer un recurso ante la Unidad de Transparencia (art. 94).

c. Derechos tutelados

Se protegerán los derechos ARCO; esto es acceso, rectificación, cancelación u oposición.

d. Procedencia

Podrá impugnarse la resolución del recurso de revisión emitido por el organismo garante ante el Instituto, mediante el recurso de inconformidad. Este recurso podrá presentarse ante el organismo garante que haya emitido la resolución o ante el Instituto, dentro del plazo de quince días contados a partir del siguiente a la fecha de la notificación de la resolución impugnada. Los organismos garantes deberán remitir el recurso de inconformidad al Instituto al día siguiente de haberlo recibido; así como las

constancias que integren el procedimiento que haya dado origen a la resolución impugnada, el cual resolverá allegándose de los elementos que estime convenientes (art. 117).

El recurso de inconformidad procederá contra las resoluciones emitidas por los organismos garantes de las entidades federativas que: clasifiquen los datos personales sin que se cumplan las características señaladas en las leyes; determinen su inexistencia, o declaren la negativa, es decir, se entreguen datos personales incompletos o que no correspondan con los solicitados; se niegue el acceso, rectificación, cancelación u oposición; se entregue o ponga a disposición en un formato incomprensible; el titular esté inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales, o se oriente a un trámite específico que no cumpla con los plazos (art. 118).

El recurso de inconformidad podrá ser desechado por improcedente cuando: sea extemporáneo, el Instituto anteriormente haya resuelto en definitiva sobre la materia del mismo; se esté tramitando ante el Poder Judicial algún recurso o medio de defensa interpuesto; el inconforme amplíe su solicitud en el recurso de inconformidad, únicamente respecto de los nuevos contenidos (art. 125).

e. Procedimiento

El escrito de interposición del recurso de inconformidad contendrá: el área responsable ante la cual se presentó la solicitud para el ejercicio de los derechos ARCO; el organismo garante que emitió la resolución impugnada; el nombre del titular que recurre o de su representante y, en su caso, del tercero interesado, así como su domicilio o el medio que señale para recibir notificaciones; la fecha en que fue notificada la resolución al titular; el acto que se recurre y los puntos petitorios, así como las razones o motivos de inconformidad; en su caso, copia de la resolución que se impugna y de la notificación correspondiente, y los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.

El promovente podrá acompañar su escrito con las pruebas y demás elementos que considere procedentes someter a juicio del Instituto (art. 119).

El Instituto resolverá el recurso de inconformidad en un plazo que no podrá exceder de treinta días, contados a partir del día siguiente de la interposición del recurso de inconformidad; plazo que podrá ampliarse por una sola vez y hasta por un período igual (art.120).

Una vez concluida la etapa probatoria, el Instituto pondrá a disposición de las partes las actuaciones del procedimiento y les otorgará un plazo de cinco días para que formulen alegatos contados a partir de la notificación del acuerdo al que se refiere este artículo (art. 123).

Las resoluciones del Instituto podrán: sobreseer o desechar el recurso de inconformidad; confirmar la resolución del organismo garante; revocar o modificar la resolución del organismo garante, u ordenar la entrega de los datos personales, en caso de omisión del responsable (art. 124).

En los casos en que mediante el recurso de inconformidad se modifique o revoque la resolución del organismo garante, este deberá emitir un nuevo fallo atendiendo los lineamientos que se fijaron al resolver la inconformidad, dentro del plazo de quince días, contados a partir del día siguiente al en que se hubiere notificado o se tenga conocimiento de la resolución dictada en la inconformidad (art.127).

Las resoluciones establecerán los plazos y términos para su cumplimiento y los procedimientos para asegurar su ejecución. Los organismos garantes deberán informar al Instituto sobre el cumplimiento de sus resoluciones. Si el Instituto no resuelve dentro del plazo la resolución que se recurrió, se entenderá confirmada. Cuando el Instituto determine que se pudo haber incurrido en una probable responsabilidad por el incumplimiento a las obligaciones previstas en la presente ley, deberá ponerlo en conocimiento del órgano interno de control o de la instancia competente para que inicie el procedimiento de responsabilidad. Las medidas de apremio resultarán aplicables para efectos del cumplimiento de las resoluciones que recaigan a los recursos de inconformidad. Estas medidas de apremio deberán establecerse en la propia resolución (art. 124).

El recurso de inconformidad solo podrá ser sobreseído cuando: el recurrente se desista expresamente; el recurrente fallezca; el organismo garante modifique o revoque su respuesta de tal manera que el recurso de inconformidad quede sin materia, o admitido el recurso, se actualice alguna causal de improcedencia en los términos de la presente ley (art. 126).

n) De la atracción de los recursos de revisión

Solo para datos personales en poder de sujetos obligados, esto es el ámbito público, el Pleno del Instituto, cuando así lo apruebe la mayoría de sus comisionados, de oficio o a petición fundada de los organismos garantes, podrá ejercer la facultad de atracción para conocer de aquellos recursos de revisión pendientes de resolución en materia de protección de datos personales, que por su interés y trascendencia, relevancia, novedad o complejidad su resolución puede repercutir de manera sustancial en la solución de casos futuros para garantizar la tutela efectiva del derecho de protección de datos (art. 131) y cuya competencia original corresponde a los organismos garantes.

Los recurrentes también podrán poner en conocimiento del Instituto la existencia de recursos de revisión, y para su conocimiento deberá cumplir con lineamientos y criterios generales de observancia obligatoria y en los cuales se considerará: la finalidad del tratamiento de los datos personales; el número y tipo de titulares involucrados en el tratamiento de datos personales llevado a cabo por el responsable; la sensibilidad de los datos personales tratados; las posibles consecuencias que se derivarían de un tratamiento indebido o indiscriminado de datos personales, y la relevancia del tratamiento de datos personales, en atención al impacto social o económico del mismo y del interés público para conocer del recurso de revisión atraído (art. 130).

o) Del recurso de revisión en materia de seguridad nacional

El Consejero Jurídico del Gobierno Federal podrá interponer el recurso de revisión en materia de seguridad nacional directamente ante la Suprema Corte de Justicia de la Nación, cuando considere que las resoluciones emitidas por el Instituto ponen en peligro

la seguridad nacional. El recurso deberá interponerse durante los siete días siguientes a aquel en el cual el organismo garante notifique la resolución al sujeto obligado. La Suprema Corte de Justicia de la Nación determinará, de inmediato, en su caso, la suspensión de la ejecución de la resolución, y dentro de los cinco días siguientes a la interposición del recurso resolverá sobre su admisión o improcedencia (art. 139).

p) De los criterios de interpretación

El Instituto podrá emitir los criterios de interpretación que estime pertinentes derivados de resoluciones que hayan causado estado, que serán de carácter orientador para los organismos garantes, y que se establecerán por reiteración al resolver tres casos análogos de manera consecutiva en el mismo sentido, por al menos dos terceras partes del Pleno del Instituto (art. 144).

q) Del procedimiento de verificación

El Instituto y los organismos garantes, en el ámbito de sus respectivas competencias, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente ley y demás ordenamientos que se deriven de esta (art. 146).

Para lo cual, podrán iniciar: de oficio cuando el Instituto o los organismos garantes cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes, o por denuncia del titular cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la presente ley; o cuando cualquier persona tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente ley. El derecho a presentar una denuncia precluye en el término de un año contado a partir del día siguiente en que se realicen los hechos u omisiones materia de la misma. Cuando los hechos u omisiones sean de tracto sucesivo, el término empezará a contar a partir del día hábil siguiente al último hecho realizado. La verificación no procederá en los supuestos de procedencia del recurso de revisión o inconformidad previstos en la presente ley (art. 147).

Los responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto o los organismos garantes, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente ley (art. 151).

r) Habeas data

El doctor Marcos Francisco del Rosario, catedrático de la Universidad Panamericana, presenta el tema del habeas data. Desafortunadamente –señala con atino el doctor del Rosario–, la configuración constitucional del esquema de protección de datos personales si bien tiene un avance significativo, como previamente se mencionó, no puede hablarse de una verdadera protección. En consecuencia, México mediante la Ley Federal de Protección de Datos Personales en Posesión de los Particulares no crea un mecanismo especializado de habeas data. Así lo sostiene el mismo autor al negar que la tutela respecto de violaciones a los datos personales, derivado de actos de autoridad, cuente con un procedimiento constitucional ex profeso y, por tanto, remite su eficacia a la vía

contenciosa administrativa. Agrega también que un juicio de amparo como mecanismo de control constitucional, utilizado para la protección de ciertos derechos incluidos los datos personales, no es propiamente hablar de habeas data en sentido estricto; de ahí que mejor dicho, la eficacia del Poder Legislativo ha sido parcial a la hora de reglamentar y establecer los alcances del derecho que estudiamos.[1450]

La ley LFTAIP, reformada en 2017, ni la LGTAIP de 2015, ni la LFPDPPP de 2010 no determinan procedimiento de *habeas data* ni hacen remisión directa a juicio de amparo dirigido al derecho a la protección de datos personales.

Ahora bien, respecto de la LGPDPPSO de 2017, esta norma si menciona como acción no administrativa sino de carácter jurisdiccional, pero no de carácter constitucional, para la defensa del derecho a la protección de datos personales.

En ese sentido, las resoluciones del Instituto y de los organismos garantes respecto de recursos de revisión serán vinculantes, definitivas e inatacables para los responsables. Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación, mediante el juicio de amparo (art. 115).

Tratándose de las resoluciones a los recursos de revisión de los organismos garantes de las entidades federativas, los particulares podrán optar por acudir ante el Instituto interponiendo el recurso de inconformidad previsto en esta ley o ante el Poder Judicial de la Federación, mediante el juicio de amparo (art. 116).

Las resoluciones del Instituto respecto de recursos de inconformidad serán vinculantes, definitivas e inatacables para los responsables y los organismos garantes. Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación, mediante el juicio de amparo (art. 129).

s) Juicio de amparo

La Ley de Amparo, reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos, cuyas últimas modificaciones corresponden al 17 de junio de 2016,[1451] regula el juicio de amparo.

t) Sujeto activo

El quejoso, persona natural o jurídica, por sí, por su representante legal o por su apoderado (art. 6), que aduce ser titular de un derecho subjetivo o de un interés legítimo individual o colectivo, siempre que alegue que la norma, acto u omisión reclamados violan los derechos constitucionales y con ello se produzca una afectación real y actual a su esfera jurídica, ya sea de manera directa o en virtud de su especial situación frente

[1450] G. RINCÓN Y A. CRISTINA, "Los datos personales en México: Perspectivas y retos de su manejo en posesión de particulares", *Cuestiones constitucionales*, 28, 2013, accedido 2 de agosto de 2017, http://www.scielo.org.mx/scielo.php?script=sci_abstract&pid=S1405-91932013000100014&lng=es&nrm=iso&tlng=es.

[1451] Cámara de Diputados del H. Congreso de la Unión, "Ley de Amparo, Reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos", accedido 24 de agosto de 2017, http://www.diputados.gob.mx/LeyesBiblio/pdf/LAmp_170616.pdf.

al orden jurídico. Es precisamente el caso de las transgresiones que pueden ocurrir por parte de sujetos obligados respecto del derecho a la protección de datos personales (art. 5).

El menor de edad, persona con discapacidad o mayor sujeto a interdicción podrá pedir amparo por sí o por cualquier persona en su nombre sin la intervención de su legítimo representante cuando este se halle ausente, se ignore quién sea, esté impedido o se negare a promoverlo. El órgano jurisdiccional le nombrará un representante especial para que intervenga en el juicio, debiendo preferir a un familiar cercano, salvo cuando haya conflicto de intereses o motivos que justifiquen la designación de persona diversa. Si el menor hubiere cumplido catorce años, podrá hacer la designación de representante en el escrito de demanda (art. 8).

En caso de fallecimiento del quejoso o del tercero interesado, siempre que lo planteado en el juicio de amparo no afecte sus derechos estrictamente personales, el representante legal del fallecido continuará el juicio en tanto interviene el representante de la sucesión (art. 16).

u) Sujetos pasivos u obligados

La autoridad responsable, aquella que dicta, ordena, ejecuta o trata de ejecutar el acto que crea, modifica o extingue situaciones jurídicas en forma unilateral y obligatoria; u omita el acto que de realizarse crearía, modificaría o extinguiría dichas situaciones jurídicas, independientemente de su naturaleza formal. Para los efectos de esta ley, los particulares tendrán la calidad de autoridad responsable cuando realicen actos equivalentes a los de autoridad, que afecten derechos en los términos de esta fracción, y cuyas funciones estén determinadas por una norma general (art. 5). En el caso, las negativas de acceso, rectificación, cancelación u oposición no justificadas conforme la ley determinan actos susceptibles de juicio de amparo.

v) Derechos tutelados por el habeas data

Todos aquellos derechos humanos reconocidos para su protección por la Constitución Política de los Estados Unidos Mexicanos, así como por los tratados internacionales de los que el Estado mexicano sea parte (art. 1), entre ellos los constantes en los artículos 6 y 16.

w) Procedencia

El juicio de amparo tiene por objeto resolver toda controversia que se suscite por normas generales, actos u omisiones de autoridad que violen los derechos humanos reconocidos y las garantías otorgadas para su protección por la Constitución Política de los Estados Unidos Mexicanos, así como por los tratados internacionales de los que el Estado mexicano sea parte (art. 1). Es precisamente aplicable a sujetos obligados que incumplan sus obligaciones de garantía y respeto del derecho a la protección de datos personales.

La norma admite que mediante el amparo también puede protegerse a las personas frente a normas generales, actos u omisiones por parte de particulares en los casos señalados en la presente ley.

x) Procedimiento del habeas data

Dentro del plazo de veinticuatro horas, contado desde que la demanda fue presentada, el órgano jurisdiccional deberá resolver si desecha, previene o admite (art. 112).

De no existir prevención, o cumplida esta, el órgano jurisdiccional admitirá la demanda; señalará día y hora para la audiencia constitucional, que se celebrará dentro de los treinta días siguientes; pedirá informe con justificación a las autoridades responsables; ordenará correr traslado al tercero interesado; y, en su caso, tramitará el incidente de suspensión. Cuando a criterio del órgano jurisdiccional exista causa fundada y suficiente, la audiencia constitucional podrá celebrarse en un plazo que no podrá exceder de otros treinta días (art. 115).

La autoridad responsable deberá rendir su informe con justificación por escrito o en medios magnéticos dentro del plazo de quince días, con el cual se dará vista a las partes (art. 117).

Las audiencias serán públicas y abiertas; se procederá a la relación de constancias, videograbaciones analizadas íntegramente, pruebas y los alegatos por escrito que formulen las partes; acto continuo se dictará el fallo que corresponda (art. 124).

De la sentencia dictada solo se admitirán los recursos de revisión, queja y reclamación; y tratándose del cumplimiento de sentencia, el de inconformidad (art. 80).

y) Institucionalidad de protección

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[1452] es el organismo cuya finalidad es la de dirigir y coordinar el Sistema Nacional de Transparencia, por intermedio de su Presidente, quien además lo es también del Consejo Nacional del Sistema.

La normativa que determina el nacimiento de este organismo es la Constitución mexicana en el artículo 6, literal A, fracción VIII, reformada en el 2009[1453] que declara respecto de la entidad encargada de velar los datos personales en manos de entidades públicas lo siguiente:

> VIII. La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley. El organismo autónomo previsto en esta fracción, se regirá por la ley en materia de transparencia y acceso a la información

[1452] "INAI | Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales", Sitio web institucional del INAI | Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, accedido 2 de octubre de 2017, http://www.snt.org.mx/index.php/component/content/category/2-uncategorised.

[1453] Congreso General de los Estados Unidos Mexicanos, "Decreto No. 59, de 29 de enero de 2016, por el que se declaran reformadas y derogadas diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de la reforma política de la Ciudad de México".

> pública y protección de datos personales en posesión de sujetos obligados, en los términos que establezca la ley general que emita el Congreso de la Unión para establecer las bases, principios generales y procedimientos del ejercicio de este derecho. En su funcionamiento se regirá por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

Por su parte, fracción I del artículo 116 de la Constitución señala que los poderes de los Estados que integran los Estados Unidos mexicanos se sujetarán a las Constituciones de los estados que por su parte establecerán organismos autónomos, especializados, imparciales y colegiados, responsables de garantizar el derecho de acceso a la información y de protección de datos personales en posesión de los sujetos obligados, conforme a los principios y bases establecidos por el artículo 6o. de esta Constitución y la ley general que emita el Congreso de la Unión para establecer las bases, principios generales y procedimientos del ejercicio de este derecho. Fracción adicionada: DOF 07-02-2014.[1454]

> En el Decreto No. 47 de 7 de febrero de 2014, por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, aparece la transitoria Séptima que determina como instancia responsable encargada de atender los temas en materia de protección de datos personales en posesión de particulares, al organismo garante establecido en el artículo 6o. de la Constitución mexicana.[1455]

z) Régimen sancionador

Ni la ley LFTAIP, reformada en 2017 ni la LGTAIP de 2015 establecen un régimen sancionador dirigido al derecho a la protección de datos personales.

Ahora bien, en la LFPDPPP de 2010 se delimita expresamente un procedimiento de imposición de sanciones, que con motivo del procedimiento de protección de derechos o del procedimiento de verificación que realice el Instituto, cuando existiere indicios de un presunto incumplimiento se iniciará este procedimiento, a efecto de determinar la sanción que corresponda (art. 61).

Las *infracciones* en cumplimiento del principio de legalidad constan en el artículo 63 de la ley analizada y consisten en las siguientes conductas llevadas a cabo por el responsable que de manera general incumplen con los derechos propios y principios aplicables a los datos personales como no cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada. Como por ejemplo: declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable; dar tratamiento a los datos personales en contravención a los principios; omitir en el aviso de privacidad; mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares; no cumplir con el apercibimiento; cambiar sustancialmente la finalidad originaria del tratamiento

[1454] Congreso General de los Estados Unidos Mexicanos, "Decreto No. 47, de 7 de febrero de 2014, por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia".
[1455] Ibíd.

de los datos; transferir datos a terceros sin comunicar a estos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos; vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable; recabar o transferir datos personales sin el consentimiento expreso del titular; recabar datos en forma engañosa y fraudulenta; obstruir los actos de verificación de la autoridad; continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares, entre otros.

Las *sanciones* se tipifican en el artículo 64, las cuales van desde el apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular, en los términos previstos por esta ley, hasta multas que van desde 100 a 160,000 hasta 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. Tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

Finalmente, el capítulo XI de la ley, tipifica los "Delitos en materia del tratamiento indebido de datos personales", por los cuales impone penas de prisión que van desde tres meses hasta cinco años, y en el caso de datos sensibles hasta el doble (art. 69) cuando el que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia (art. 67) o con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos (art. 68).

En la LGPDPPSO de 2017 también consta un régimen sancionador que empieza con la determinación de medidas de apremio por las cuales el Instituto y los organismos garantes podrán imponer medidas de apremio para asegurar el cumplimiento de sus determinaciones, por ejemplo: amonestación pública, o multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización.

El incumplimiento de los sujetos obligados será difundido en los portales de obligaciones de transparencia del Instituto y los organismos garantes, considerados en las evaluaciones que realicen estos. En caso de que el incumplimiento de las determinaciones del Instituto y los organismos garantes implique la presunta comisión de un delito o una de las conductas señaladas en el artículo 163 de la presente ley, deberán denunciar los hechos ante la autoridad competente. Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos (art. 153).

Si a pesar de la ejecución de las medidas de apremio, previstas en el artículo anterior, no se cumpliere con la resolución, se requerirá el cumplimiento al superior jerárquico para que en el plazo de cinco días lo obligue a cumplir sin demora. De persistir el incumplimiento, se aplicarán sobre aquellas medidas de apremio establecidas en el artículo anterior. Transcurrido el plazo, sin que se haya dado cumplimiento, se dará vista la autoridad competente en materia de responsabilidades (art. 154).

Para calificar las medidas de apremio establecidas en el presente capítulo, el Instituto y los organismos garantes deberán considerar: la gravedad de la falta del responsable, determinada por elementos tales como el daño causado; los indicios de intencionalidad; la duración del incumplimiento de las determinaciones del Instituto o los organismos

garantes y la afectación al ejercicio de sus atribuciones; la condición económica del infractor, y la reincidencia (art. 157).

En caso de reincidencia, el Instituto o los organismos garantes podrán imponer una multa equivalente de hasta el doble de la que se hubiera determinado por el Instituto o los organismos garantes. Se considerará reincidente al que, habiendo incurrido en una infracción que haya sido sancionada, cometa otra del mismo tipo o naturaleza (art. 158).

Las multas que fijen el Instituto y los organismos garantes se harán efectivas por el Servicio de Administración Tributaria o las Secretarías de Finanzas de las Entidades Federativas, según corresponda, mediante los procedimientos que las leyes establezcan (art. 156).

En el artículo 163 constan descritas las sanciones por incumplimiento de las obligaciones de los responsables, como por ejemplo: actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO; incumplir los plazos de atención previstos en la presente ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate; usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión; dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente ley; no contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la presente ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia; clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción solo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales; incumplir el deber de confidencialidad; no establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la presente ley; presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la presente ley; llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente ley; obstruir los actos de verificación de la autoridad; crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente ley; no acatar las resoluciones emitidas por el Instituto y los organismos garantes, y omitir la entrega del informe anual y demás informes.

En caso de que el incumplimiento de las determinaciones de los organismos garantes implique la presunta comisión de un delito, el organismo garante respectivo deberá denunciar los hechos ante la autoridad competente (art. 168).

aa) Transferencia internacional de datos personales

La ley LFTAIP, reformada en 2017, ni la LGTAIP de 2015 no señalan aspecto alguno sobre la transferencia internacional de datos personales.

Acerca de la LFPDPPP de 2010, consta el capítulo V, “De la transferencia de datos” por el cual el responsable que pretenda transferir los datos personales a terceros nacionales

o extranjeros, distintos del encargado, deberá comunicar a estos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos; de igual manera, el tercero receptor asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos (art. 36).

Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular, entre otras, cuando la transferencia esté prevista en una ley o tratado en los que México sea parte; sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios; sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas; sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero; sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia; sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular (art. 37)

Ahora bien, respecto de la LGPDPPSO de 2017, aparece la *remisión*, concepto que no consta en la LFPDPPP de 2010 y que se refiere a que toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano; mientras que la *transferencia* es toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

En esta ley, el título de las comunicaciones de datos personales en el Capítulo Único "De las transferencias y remisiones de datos personales" determina que toda transferencia de datos personales, sea esta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones legales (art. 65). Además, se determinará cuando no es necesario el consentimiento tal como señala la normativa aplicable a particulares.

Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes (art. 66).

bb) De las versiones públicas

En la LFTAIP, reformada en 2017, consta la posibilidad de que cuando un documento o expediente contenga partes o secciones reservadas o confidenciales, los sujetos obligados por medio de sus áreas, para efectos de atender una solicitud de información, deberán elaborar una versión pública en la que se testen las partes o secciones clasificadas, indicando su contenido de manera genérica, fundando y motivando su clasificación, en términos de lo que determine el Sistema Nacional (art. 118). Si bien esta norma es aplicable a transparencia y acceso a la información pública, también

puede ser aplicable en aquellos casos en los que un documento contiene datos públicos y datos personales por ejemplo las sentencias judiciales.

cc) Código de conducta

La LFPDPPP de 2010 determina que las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la presente ley. Dichos esquemas deberán contener mecanismos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas eficaces en caso de incumplimiento. Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos y contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares. Dichos esquemas serán notificados de manera simultánea a las autoridades sectoriales correspondientes y al Instituto (art. 44).

dd) De la portabilidad de los datos

La LFPDPPP de 2010 señala que cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

El Sistema Nacional establecerá mediante lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales (art. 57).

ee) Acciones preventivas en materia de protección de datos personales

La LGPDPPSO de 2017 declara que para el cumplimiento de las obligaciones previstas en la presente ley, el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas que tengan por objeto: elevar el nivel de protección de los datos personales; armonizar el tratamiento de datos personales en un sector específico; facilitar el ejercicio de los derechos ARCO por parte de los titulares; facilitar las transferencias de datos personales; complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales, y demostrar ante el Instituto o, en su caso, los organismos garantes, el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales (art. 72).

Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una evaluación de impacto en la protección de datos personales, y presentarla ante el Instituto o los organismos garantes, según corresponda, los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales (art. 74).

2.14 Uruguay (2008)

La Constitución Política de la República Oriental del Uruguay de 1967 únicamente contiene dentro de sus preceptos lo estipulado en el artículo 7:

> Artículo 7°.- Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad. Nadie puede ser privado de estos derechos sino conforme a las leyes que se establecieron por razones de interés general.[1456]

Normas relacionadas son: el artículo 11 que se refiere a inviolabilidad de domicilio y el artículo 28 relativo a la inviolabilidad de correspondencia epistolar, telegráfica o de cualquier otra especie.

Ahora bien, el artículo 72 señala que la enumeración de derechos, deberes y garantías hecha por la Constitución no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno. En consecuencia, es posible invocar el derecho a la protección de datos personales en virtud de esta cláusula abierta en garantía de los derechos fundamentales.

Por eso se aprobó la Ley 18.331, de Protección de Datos Personales y Acción de Habeas Data, 11 de agosto de 2008,[1457] en cuyo artículo 1º determina que la protección de datos personales es un derecho humano inherente a la persona, que está comprendido en el artículo 72 de la Constitución de la República.

Días después se dictó el Decreto Reglamentario 414/009, 31 de agosto de 2008, que Reglamenta la Ley de Protección de Datos Personales.[1458]

Como norma sectorial de importancia consta la Ley 18.381, 7 de noviembre de 2008, de Acceso a la Información Pública.[1459]

[1456] "Uruguay: Constitución Política de la República Oriental del Uruguay de 1967 con Reformas hasta 2004", *Political Database of the Americas*, 1967, accedido 25 de agosto de 2017, http://pdba.georgetown.edu/Constitutions/Uruguay/uruguay04.html.

[1457] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, "Ley Nº 18.331, de Protección de Datos Personales y Acción de *Habeas Data*, de 11 de agosto de 2008", *República Oriental del Uruguay, Poder Legislativo*, 2008, accedido 25 de agosto de 2017, https://parlamento.gub.uy/documentosyleyes/leyes?Ly_Nro=18331&Ly_fechaDePromulgacion%5Bmin%5D%5Bdate%5D=&Ly_fechaDePromulgacion%5Bmax%5D%5Bdate%5D=&Ltemas=&tipoBusqueda=T&Searchtext=.

[1458] Presidencia de la República Oriental del Uruguay, "Decreto N° 414/009, de 31 agosto de 2009, Reglamenta la Ley de Protección de Datos Personales", *Agesic*, 2009, accedido 25 de agosto de 2017, https://www.agesic.gub.uy/innovaportal/v/295/1/agesic/decreto-n%C2%B0-414_009-de-31-agosto-de-2009.html.

Asimismo, se dictó el Decreto 664/008, 22 de diciembre de 2008, que crea el Registro de Bases de Datos Personales, adscrito a la URCDP.[1460]

En la Decisión de Ejecución 2012/484/UE, 21 de agosto de 2012, de la Comisión de la Unión Europea, se declaró a Uruguay como país adecuado para el tratamiento de datos personales, es decir que cumple con la dispuesto en la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Uruguay fue el segundo país latinoamericano en tener este reconocimiento,[1461] que fuera modificado en virtud de la sentencia Schrems para sustituir las disposiciones que limitaban las facultades de las autoridades nacionales de supervisión y ampliarlas; además se impuso la obligación de comprobar periódicamente si la conclusión relativa a la adecuación del nivel de protección ofrecido por el tercer país en cuestión, aún era objetiva y jurídicamente justificada. A la luz de las conclusiones de la sentencia, en lo que se refiere al acceso a los datos personales por parte de las autoridades públicas, también debe hacerse un seguimiento de las normas y prácticas que regulen dicho acceso, por medio de Decisión de Ejecución (UE) 2016/2295 de la Comisión, 16 de diciembre de 2016, por la que se modificaron las Decisiones 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE, 2011/61/UE, y las Decisiones de Ejecución 2012/484/UE y 2013/65/UE, relativas a la protección adecuada de los datos personales por determinados países, en aplicación del artículo 25, apartado 6, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.[1462]

Mediante la Ley 19.030 de 27 de diciembre de 2012, publicada el 7 de enero de 2013, Uruguay ratifica el Convenio Nº108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, adoptado en Estrasburgo, y el Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos

---

[1459] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, "Ley N° 18.381, de 7 de noviembre de 2008 de Acceso a la Información Pública", *República Oriental del Uruguay, Poder Legislativo*, 2008, accedido 25 de agosto de 2017, https://parlamento.gub.uy/documentosyleyes/leyes?Ly_Nro=18381&Ly_fechaDePromulgacion%5Bmin%5D%5Bdate%5D=&Ly_fechaDePromulgacion%5Bmax%5D%5Bdate%5D=&Ltemas=&tipoBusqueda=T&Searchtext=.

[1460] Presidencia de la República Oriental del Uruguay, "Decreto N° 664/008, de 22 de diciembre de 2008 que crea el Registro de Bases de Datos Personales, adscrito la URCDP", *Banco Central del Uruguay*, 2008, accedido 25 de agosto de 2017, http://www.bcu.gub.uy/Leyes%20y%20Decretos/Decreto-664-2008.pdf.

[1461] La Comisión Europea, "Decisión de Ejecución 2012/484/UE, de 21 de agosto de 2012, de la Comisión de la Unión Europea de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales [notificada con el número C(2012) 5704] (Texto pertinente a efectos del EEE) (2012/484/UE)", *EUR-Lex*, accedido 25 de agosto de 2017, http://eur-lex.europa.eu/legal-content/ES/TXT/?toc=OJ%3AL%3A2012%3A227%3ATOC&uri=uriserv%3AOJ.L_.2012.227.01.0011.01.SPA.

[1462] La Comisión Europea, "Decisión de Ejecución (UE) 2016/2295 de la Comisión, de 16 de diciembre de 2016, por la que se modifican las Decisiones 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE, 2011/61/UE, y las Decisiones de Ejecución 2012/484/UE y 2013/65/UE, relativas a la protección adecuada de los datos personales por determinados países, en aplicación del artículo 25, apartado 6, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo [notificada con el número C(2016) 8353] (Texto pertinente a efectos del EEE)".

adoptado en Estrasburgo, el 8 de noviembre de 2001. Dicha norma entra en vigencia el 1 de agosto de 2013, de esta forma Uruguay se convierte en el primer país de Latinoamérica en firmar este Convenio.[1463]

Adicionalmente, la Ley N° 19355 de Presupuesto nacional de sueldos gastos e inversiones. Ejercicio 2015 – 2019 promulgado el 19 de diciembre de 2015 y publicado el 30 de diciembre de 2015[1464] establece reformas a la Ley N° 18.331 sobre la confidencialidad de las historias clínicas y la licitud del tratamiento, sin necesidad de autorización del titular, de registros y documentos destinados a la protección y contralor del trabajo.

Finalmente, con la entrada en vigencia del Reglamento General de Protección de Datos Personales, la Ley N° 19670 de aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2017[1465], promulgada el 15 de octubre de 2018 y publicado el 25 de octubre de 2018 dispone las reformas normativas necesaria para mantener el nivel adecuado de protección y fortalecer la protección de datos personales.

A efectos de la identificación del contenido esencial se realizará el análisis de la Ley 18.331, de Protección de Datos Personales y Acción de Habeas Data, 11 de agosto de 2008 (en adelante la Ley 18.331), con sus reformas y de ser el caso el Decreto Reglamentario 414/009, 31 de agosto de 2008, que Reglamenta la Ley de Protección de Datos Personales, por ser de aplicación general (en adelante Decreto 414/009). Las otras normas invocadas por su carácter sectorial no reflejan el ámbito necesario para categorizar lo elemental del derecho por lo que no serán analizadas:

a) Ámbito: Registros o ficheros públicos y privados

La norma uruguaya, Ley 18.331 y el Decreto 414/009 determinan la aplicabilidad de la regulación que protege los datos personales, tanto a bases de datos del ámbito público como del privado (art. 2 en las dos normativas).

Tanto la Ley 18.331 como el Decreto 414/009 señalan las bases de datos a las que no se deberá aplicar la presente ley:

[1463] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, "Ley Nº 19.030 aprobación del Convenio Nº 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos", *República Oriental del Uruguay, Poder Legislativo*, 2012, accedido 25 de agosto de 2017, https://parlamento.gub.uy/documentosyleyes/leyes?Ly_Nro=19030&Ly_fechaDePromulgacion%5Bmin%5D%5Bdate%5D=&Ly_fechaDePromulgacion%5Bmax%5D%5Bdate%5D=&Ltemas=&tipoBusqueda=T&Searchtext=.

[1464] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, "Ley N° 19355 de Presupuesto nacional de sueldos gastos e inversiones. Ejercicio 2015 – 2019", Centro de Información Oficial, accedido el 30 de agosto de 2019, https://www.impo.com.uy/bases/leyes/19355-2015

[1465] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, "Ley N° 19670 de aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2017", Centro de Información Oficial, accedido el 30 de agosto de 2019, https://www.impo.com.uy/bases/leyes/19670-2018

A) A las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, entendiéndose por éstas las que se desarrollan en un ámbito estrictamente privado, entre otros, los archivos de correspondencia y agendas personales.

B) Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.

C) Las bases de datos creadas y reguladas por leyes especiales (art. 2).

Respecto de la territorialidad el artículo 3º del Decreto 414/009 señala que los tratamientos de datos personales están sometidos a la ley uruguaya cuando sean efectuados por un responsable establecido, que ejerza su actividad, o use medios situados en territorio uruguayo, excepto que los citados medios utilicen exclusivamente fines de tránsito.

La Ley No. 19.670 reforma la Ley N° 19355 que regula a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), en el Proyecto Trámites en Línea, que tiene por finalidad promover y desarrollar estrategias de simplificación de trámites.

La citada Ley No. 19.670 a través de su artículo 37 dispone que las entidades públicas, cuando realicen el tratamiento de datos personales, en su obligación de simplificar sus trámites, "estarán sometidas a la Ley N° 18.331, de 11 de agosto de 2008 –sobre protección de datos personales– y sus modificativas y concordantes".

Además, esta norma también complementa el régimen dispuesto en la Ley 18.331 de protección de datos personales, ya que señala que por el ámbito subjetivo es aplicable al responsable o encargado de tratamiento establecido en el Uruguay, o que ejerce su actividad en el país.

Pero además, en el caso de que no esté establecido en territorio uruguayo, la Ley 18.331 regirá cuando: las actividades del tratamiento están relacionadas con la oferta de bienes o servicios dirigidos a habitantes de la República o con el análisis de su comportamiento; si lo disponen normas de derecho internacional público o un contrato; si en el tratamiento se utilizan medios situados en el país.

De lo transcrito, se colige que se ha adoptado el modelo europeo de extraterritorialidad, por el cual la normativa de protección de datos personales puede aplicarse a responsables de tratamiento o encargados que se encuentren fuera del país siempre que oferten bienes a habitantes al territorio nacional. Además, cobra relevancia el énfasis añadido por la norma respecto de la aplicación de la norma de protección de datos si el responsable realiza análisis de comportamiento de las personas, como visible mecanismo que pretende evitar posibles vulneraciones o manipulaciones de los ciudadanos uruguayos asociados a elementos como la voluntad o el ejercicio de sus libertades.

Finalmente, la norma exceptúa los casos en que "los medios se utilicen exclusivamente con fines de tránsito, siempre que el responsable del tratamiento designe un representante, con domicilio en territorio nacional, ante la Unidad Reguladora y de Control de Datos Personales." De esta manera, se deja por fuera del ámbito de

aplicación de la normativa de protección de datos personales a los datos de tránsito, siempre y cuando se registre al responsable, esto con la finalidad de establecer un control mínimo que pueda activarse en el caso de producirse alguna vulneración.

b) Naturaleza del dato

Ley 18.331 sobre definiciones determina que se entiende por dato personal aquella información de cualquier tipo referida a personas físicas o jurídicas, determinadas o determinables (art. 4).

La normativa reconoce varios tipos de datos: el dato sensible, datos personales relativos a la comisión de infracciones penales, civiles o administrativas, relativos a salud, telecomunicaciones, o bases de datos con fines de publicidad.

Por dato sensible se comprende aquel que revela origen racial y étnico, preferencia política, convicción religiosa o moral, afiliación sindical e informaciones referentes a la salud o a la vida sexual (art. 4). Solo pueden ser recolectados y tratados por razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal o sean tratados con finalidades estadísticas o científicas y siempre que se disocien de sus titulares. Queda prohibida la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles. Se exceptúan aquellos que posean los partidos políticos, sindicatos, iglesias, confesiones religiosas, asociaciones, fundaciones y otras entidades sin fines de lucro, cuya finalidad sea política, religiosa, filosófica, sindical, que hagan referencia al origen racial o étnico, a la salud y a la vida sexual, acerca de los datos relativos a sus asociados o miembros, sin perjuicio que la comunicación de dichos datos precisará siempre el previo consentimiento del titular del dato (art. 18).

Los datos personales relativos a la comisión de infracciones penales, civiles o administrativas solo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de la ley (art. 18).

Respecto a datos relativos a la salud física o mental, pasada, "presente y futura de una persona o su porcentaje de discapacidad o a su información genética" (art. 4 D) del Decreto 414/009). Solo podrán recolectarlos los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud que acudan a los mismos o que estén o hubieren estado bajo tratamiento, respetando los principios del secreto profesional (art. 19).

Los operadores de datos relativos a las telecomunicaciones para redes públicas o para servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos personales de los usuarios (art. 20).

Sobre datos relativos a bases de datos con fines de publicidad, solo podrán tratarse para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando estos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento. El titular podrá en cualquier momento solicitar el retiro o bloqueo de sus datos de los bancos de datos a los que se refiere el presente artículo (art. 21).

Los datos relativos a la actividad comercial o crediticia solo tendrán como finalidad brindar informes objetivos de carácter comercial, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticio. Para el caso de las personas jurídicas, además de las circunstancias previstas en la presente ley (art. 22).

Respecto del tratamiento de datos se señala que consiste en aquellas operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros mediante comunicaciones, consultas, interconexiones o transferencias (art. 4).

En el Decreto 414/009 se amplían los conceptos delimitados en la Ley 18.331 y con la rúbrica de ámbito objetivo, se determina que está bajo el régimen jurídico de la protección de datos personales cualquier forma de recolección, registro, todo tipo de tratamiento, automatizado o no, bajo cualquier soporte y modalidad de uso (art. 2º) y específicamente respecto de los datos, cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo que refiera a ellas (art. 1º), en el mismo sentido, el concepto de base de datos es amplio e inclusivo, pues consiste en el conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso (Ley 18.331, art. 4).

c) Sujeto activo

De acuerdo al ámbito subjetivo de la Ley 18.331, el derecho a la protección de los datos personales se aplicará a personas naturales y por extensión a las personas jurídicas, en cuanto corresponda (art. 2º), en el mismo sentido el Decreto 414/009.

Conforme las definiciones establecidas en la ley, el titular de los datos es la persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la presente ley; esto es todo aquello que no corresponda a tratamiento doméstico o expresamente excepcionado por la ley (art. 4, lit. L); por su parte el Decreto 414/009, lo denomina *interesado* (art. 4, lit. G).

Cuando se trate de datos de personas fallecidas, el ejercicio del derecho de acceso corresponderá a cualquiera de sus sucesores universales (art. 14).

d) Sujeto pasivo

La Ley 18.331 determina, en el artículo 4 relativo a las definiciones aplicables a la ley, los siguientes sujetos pasivos que previenen todas las formas de acercamiento a los datos personales:

- Responsable de la base de datos o del tratamiento es la persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.
- Usuario de datos es toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos.

- Destinatario es la persona física o jurídica, pública o privada, que recibiere comunicación de datos, se trate o no de un tercero.
- Encargado del tratamiento es la persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento.
- Tercero es la persona física o jurídica, pública o privada, distinta del titular del dato, del responsable de la base de datos o tratamiento, del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento.

e) Objeto o bien jurídico

a. Derecho de información

La Ley 18.331 indica que el derecho de información frente a la recolección de datos se produce cuando se recaben datos personales, ya que el responsable deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca: la finalidad y destinatarios de los datos tratados, la existencia de la base de datos cualquiera sea su soporte y la identidad; el domicilio del responsable; el carácter obligatorio o facultativo de las respuestas, especialmente datos sensibles; las consecuencias de entregar o no sus datos y, de los derechos de acceso, rectificación y supresión de datos de los cuales son titulares (art. 13).

Únicamente, la ley ha autorizado a no informar cuando la información afecte a la defensa nacional, a la seguridad pública o a la persecución de infracciones penales (art. 27).

b. Autodeterminación informativa

No consta expresamente la frase autodeterminación informativa, pero el artículo 72 de la Constitución de la República estipula que la norma constitucional no excluirá otros derechos inherentes a la personalidad humana, por lo que la aprobación de la Ley 18.331, de Protección de Datos Personales y Acción de Habeas Data, 11 de agosto de 2008[1466] y la expresa mención del derecho a la protección de datos personales como un derecho humano inherente a la dignidad de persona, configura que se encuentra reconocido como autónomo e independiente y en consecuencia su contenido caracterizante, esto es la autodeterminación informativa, también se encuentra reconocida.

Todo lo dicho coincide con la declaración de Uruguay como país adecuado para el tratamiento de datos personales y con la aprobación de la Ley 19.030, 27 de diciembre de 2012, por la cual Uruguay se adhirió al Convenio 108 ante el Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos.[1467]

[1466] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, "Publicada D.O. 18 ago/008 - Nº 27549".

[1467] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, "Ley Nº 19.030 aprobación del Convenio Nº108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y

c. Necesidad de mandato legal para tratamiento sin autorización del titular

La Ley 18.331 determina que la regla es el consentimiento informado y que solo la información recogida, cumpliendo con las características propias de este, puede ser considerada lícita (art. 9º). Además indica que en el caso de datos sensibles estos solo pueden ser recolectados y tratados por razones de interés general autorizadas por ley, o si el organismo solicitante tiene mandato legal o si serán tratados con fines estadísticos o científicos y siempre que se disocien de sus titulares (art. 18); así, esta norma establece legalmente los únicos casos en los que es posible realizar el tratamiento de datos sin autorización del titular.

d. Principios

La norma uruguaya, Ley 18.331, contiene el capítulo II, denominado "Principios generales", cuyo artículo 5 determina que la actuación de los responsables de las bases de datos, tanto públicos como privados, y, en general, de todos quienes actúen en relación con datos personales de terceros, deberá ajustarse a los siguientes principios generales: legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad. Finalmente, los principios generales servirán de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de estas disposiciones.

i. Deber de información

Cuando se describe el derecho de información se determina que los responsables deberán informar previamente a sus titulares en forma expresa, precisa e inequívoca: la finalidad y destinatarios de los datos tratados, la existencia de la base de datos cualquiera sea su soporte y la identidad; el domicilio del responsable; el carácter obligatorio o facultativo de las respuestas, especialmente datos sensibles; las consecuencias de entregar o no sus datos y, de los derechos de acceso, rectificación y supresión de datos de los cuales son titulares (art. 13).

Por su parte, el Decreto 414/009 delimita la obligación de que para recolección y tratamiento de datos el consentimiento sea informado; en otras palabras, que se cumpla con el deber de información, así como con el de finalidad ya que se solicita que se conozca inequívocamente la finalidad a la que se destinarán los datos, y el tipo de actividad desarrollada por el responsable de la base de datos o tratamiento. Caso contrario, el consentimiento será nulo (art. 5).

ii. Pertinencia

No consta como principio específico. Únicamente existe una referencia en la descripción del principio de finalidad, constando que deberá eliminarse los datos que ya no fueran pertinentes a los fines para los cuales hubieren sido recolectados.

Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos".

iii. Calidad

No consta en la Ley 18.331 el principio de calidad, sino que un contenido equivalente al mismo; aparece denominado como principio de veracidad. Por el cual, para tratar datos personales deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. En consecuencia, los datos deberán ser exactos y es de cargo de responsable actualizarlos de ser necesario; si ha constatado la inexactitud o falsedad de los datos, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo, deberán ser eliminados aquellos datos que hayan caducado según lo previsto en la presente ley (art. 7).

Esta norma también menciona que la recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley; contenido que es propio del principio de legalidad o licitud, pero que consta incluido en este denominado principio de veracidad.

iv. Finalidad

De conformidad con la Ley 18.331, los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención y deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados, y por ello tampoco podrán comunicarse datos entre bases de datos, sin que medie ley o previo consentimiento informado del titular, pues es necesario que el titular conozca las nuevas finalidades a las que se pretende someter sus datos (art. 8º).

Los datos relativos a la actividad comercial o crediticia solo tendrán como finalidad brindar informes objetivos de carácter comercial, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticio. Para el caso de las personas jurídicas, además de las circunstancias previstas en la presente ley (art. 22); es decir, cualquier otra finalidad.

v. Seguridad

Conforme la Ley 18.331, el responsable o usuario de la base de datos deberá adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Estas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad (art. 10).

El Decreto 414/009, por su parte, determina quiénes deben cumplir con las medidas de seguridad cuando admite que tanto el responsable como el encargado de la base de datos o tratamiento deberán proteger los datos personales que sometan a tratamiento (art. 7º).

Así también, establece como concepto de seguridad, aquellas medidas técnicas y organizativas que resulten idóneas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales (art. 7º).

El responsable o encargado de la base de datos o tratamiento que conozca de la ocurrencia de vulneraciones de seguridad, en cualquier fase del tratamiento, y cuando sea susceptible de afectar de forma significativa los derechos de los interesados, deberá informar al titular, (art. 8º).

La Ley N° 19670 de aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2017[1468], de 25 de octubre de 2018, a través de su artículo 38 propone un texto que completa el artículo 8 de Decreto 414/009 previamente citado que dispone textualmente que:

> […] cuando el responsable o encargado de una base de datos o de tratamiento, tome conocimiento de la ocurrencia de la vulneración de seguridad, deberá informar inmediata y pormenorizadamente de ello y de las medidas que adopte, a los titulares de los datos y a la Unidad Reguladora y de Control de Datos Personales, la que coordinará el curso de acción que corresponda, con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy). La reglamentación determinará el contenido de la información correspondiente a la vulneración de seguridad.

Si bien, en la normativa uruguaya constaba la obligación del responsable de tratamiento de notificar vulneraciones de seguridad, la norma actual prevé el procedimiento aplicable, pues ya no es suficiente el aviso al titular sino que deberá notificarse a la autoridad de control y a los entes estatales encargados de la seguridad informática. La intencionalidad de la norma es establecer un sistema integral y coordinado de ciberseguridad, en el que participen actores públicos y privados.

vi. Consentimiento

La Ley 18.331 señala como definición de consentimiento del titular, toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierne (art. 4).

En virtud de este concepto, consagra como eje del sistema al principio del previo consentimiento informado, ya que el tratamiento de datos personales solo es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado. Además establece la obligación de que estas características se documenten (art. 9º).
En el Decreto 414/009 se delimita que deberá facilitarse al titular un medio sencillo, claro y gratuito para que manifieste su consentimiento o su negativa al tratamiento de sus datos.

Se entenderá cumplido tal deber cuando se permita al titular la elección entre dos opciones claramente identificadas, que no se encuentren premarcadas a favor o en contra. Vencido el plazo de diez días hábiles desde que el titular de los datos reciba la solicitud de consentimiento sin que se manifieste, su silencio equivaldrá a una negativa (art. 6º). Como se puede colegir, el consentimiento en el caso del Uruguay es expreso y no cabe el tácito.

[1468] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, "Ley N° 19670 de aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2017", Centro de Información Oficial, accedido el 30 de agosto de 2019, https://www.impo.com.uy/bases/leyes/19670-2018

vii. Limitaciones al consentimiento

La misma Ley 18.331 aclara que no será necesario el previo consentimiento cuando: los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación; se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documentos de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma; deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento; se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico (art. 9).

Finalmente, ese texto señala que respecto de datos sensibles, estos solo pueden ser tratados previo consentimiento expreso; además este debe constar por escrito del titular como garantía extra de su recolección y tratamiento (art. 18).

viii. Legalidad

Según la Ley 18.331, la formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia. Las bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública (art. 6º). De esta manera, se entiende como principio de legalidad lo que en otras obligaciones se reconoce como obligación de registro de bases de datos y que va de la mano del derecho de consulta.

ix. Reserva

La Ley 18.331 señala que aquellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros no solo del responsable, sino de sus empleados aun cuando ya no sean parte de la entidad. Esta obligación subsistirá aun después de finalizada la relación con el responsable de la base de datos (art. 11). En la legislación uruguaya aparece como principio de reserva lo que en otras normativas consta como derecho de confidencialidad.

En este caso, las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos so pena de ser responsables penalmente (art. 302, Código Penal).

No existe reserva en los casos de orden de la justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular (art. 11).

Adicionalmente, la Ley N° 19355 establece el artículo 466 por el cual, se asegurará la confidencialidad en el intercambio de información clínica en concordancia con la Ley N° 18.331.

x. Responsabilidad

En la Ley 18.331, el principio de responsabilidad, se basa en que el responsable de la base de datos lo es de las violaciones de las disposiciones de la presente ley que él no haya incentivado cumplir (art. 12).

La Ley No. 19.670 reforma la Ley 18.331 y siguiendo el modelo europeo añade al texto anterior lo relativo a la responsabilidad proactiva, por la cual:

> […] el responsable deberá adoptar medidas técnicas y organizativas apropiadas: privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, entre otras, a fin de garantizar un tratamiento adecuado de los datos personales y demostrar su efectiva implementación.

De esta manera, se introduce sin mayor desarrollo temas complejos que atienden a un modelo de protección basado en el respeto a los derechos humanos más que a la seguridad tecnológica solamente, por lo que, será la reglamentación la que determinará las medidas fácticas que permitan materializar esta disposición, para lo cual será indispensable dimensionar los "tipos de datos, tratamientos y responsables, así como la oportunidad para su revisión y actualización", artículo 12 reformado.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

a. Derecho de acceso

La Ley 18.331 determina que todo titular de datos personales, debidamente identificado, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas. Este derecho de acceso solo podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico (art. 14).

Cuando se trate de datos de personas fallecidas, el ejercicio del derecho corresponderá a cualquiera de sus sucesores universales (art. 14).

La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento solo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin (art. 14).

b. Derecho de rectificación y actualización

La Ley 18.331 estipula que toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización o inclusión de los datos personales constantes en una base de

datos, la cual se efectuará sin cargo alguno para el titular (art. 15). Proceden estos derechos al constatarse el error, la falsedad (art. 15), la inexactitud o la incompletitud (art. 10º, Decreto 414/099).

Durante el proceso de verificación, rectificación o inclusión de datos personales, ante el requerimiento de terceros por acceder a informes, se deberá dejar constancia que dicha información se encuentra sometida a revisión (art. 15).

Los responsables de las bases de datos podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando, y aquellos sobre Hacienda Pública cuando al hacerlo se obstaculicen actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias o cuando el titular del dato esté siendo objeto de actuaciones inspectivas (art. 26).

En el supuesto de comunicación o transferencia de datos, el responsable de la base de datos o del tratamiento debe notificar la rectificación, inclusión o supresión al destinatario dentro del quinto día hábil de efectuado el tratamiento del dato (art. 15).

c. Derecho de oposición

Ni en la Ley 18.331 ni en el Decreto 414/009 se determina entre los derechos el de oposición.

d. Derecho de cancelación

El artículo 4º del Decreto 414/009, cuando expone las definiciones determina varios conceptos: a) bloqueo de datos, procedimiento mediante el cual se reservan datos con el fin de impedir su tratamiento, excepto para ser puestos a disposición de los Poderes del Estado, o instituciones que estén legalmente habilitadas, a los efectos de atender las posibles responsabilidades surgidas del tratamiento; b) cancelación o supresión de datos, aquel procedimiento mediante el cual el responsable cesa en el uso de los datos; la supresión o cancelación implica el bloqueo por un plazo; vencido este se deberá proceder a su eliminación definitiva; c) cesión de datos, por el cual se comunica los datos a un tercero, dicha comunicación debe ser detenida cuando los datos se eliminan de la base original y además debe reportarse al tercero para que también los elimine de la suya.

Por su parte, la Ley 18.331 establece que no procede la eliminación o supresión de datos personales salvo en aquellos casos de: a) perjuicios a los derechos e intereses legítimos de terceros; b) notorio error o falsedad; c) contravención a lo establecido por una obligación legal (art. 15). De este modo, se distingue de la oposición, ya que para cancelar es indispensable que existan estas condiciones; mientras que la oposición se basa exclusivamente en el consentimiento del titular que es revocado en cualquier momento.

El Decreto 414/009 señala que el derecho de supresión permite al titular a que se eliminen los datos cuya utilización por terceros resulte ilegítima, o que resulten ser inadecuados o excesivos; no procederá cuando los datos personales deban ser

conservados en virtud de razones históricas, estadísticas o científicas y de acuerdo con la legislación aplicable o, en su caso, en las relaciones contractuales entre el responsable y el titular, que justificaren el tratamiento de los datos (art. 13º).

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales:

La Ley 18.331 señala que el derecho no debe verse sometido a una decisión con efectos jurídicos que le afecte de manera significativa, que se base en un tratamiento automatizado o no de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros (art. 16).

El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad. En este caso, el afectado tendrá derecho a obtener información del responsable de la base de datos, tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto. La valoración sobre el comportamiento de las personas, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado (art. 16). Comparativamente, esta es la norma que más desarrolla los mecanismos fácticos que permiten la vigencia de este derecho, especialmente por el criterio de reversión de la carga probatoria.

Adicionalmente y aunque no se refieren a valoraciones automatizadas, respecto de bases de datos crediticias, sus responsables se limitarán a realizar el tratamiento objetivo de la información registrada tal cual esta le fuera suministrada, debiendo abstenerse de efectuar valoraciones subjetivas sobre la misma (art. 22).

f. Derecho de consulta al registro general de protección de datos personales

Conforme la Ley 18.331, exclusivamente para la creación, modificación o supresión de bases de datos de carácter personal de titularidad privada, que no sean para un uso exclusivamente individual o doméstico, se ha previsto que las personas físicas o jurídicas privadas deberán registrarse (art. 28) en el Registro que al efecto habilite el Órgano de Control (art. 29). De esta forma, no consta como derecho de consulta sino como obligación de registro de los responsables de bases de datos.

Para eso, se necesitará de la identificación de la base de datos, su responsable, la naturaleza de los datos que contiene, los procedimientos de obtención y tratamiento de datos, las medidas de seguridad, los derechos de los titulares, sus procedimientos, formas y condiciones de interposición, el destino de los datos y personas físicas o jurídicas a las que pueden ser transmitidos, el tiempo de conservación de los datos (art. 29), incluidos los cinco años previstos para bases crediticias (art. 22).

Así, se controlará que ningún usuario de datos posea datos personales de naturaleza distinta a los declarados en el registro. En caso de incumplimiento podrán producirse sanciones administrativas (art. 29).

Por su parte, el Decreto 414/009 admite como actos y documentos inscribibles aquellos que provienen de bases de datos cuyos responsables sean personas jurídicas públicas, estatales o no, y no solo los de naturaleza privada. No existiendo ámbito personal o doméstico para las personas jurídicas. Además, deberán constar en el registro los códigos de conducta de práctica profesional que establezcan normas para el tratamiento de datos personales y para las autorizaciones de transferencias internacionales de datos personales (art. 15).

El plazo de inscripción será de máximo de 90 días a partir del inicio de sus actividades (art. 17º). La fecha de la inscripción se computará como fecha de inscripción definitiva, aunque la Resolución de la URCPD sea posterior. Los responsables de bases de datos de carácter personal deberán exhibir en un lugar visible y accesible a los usuarios el número y fecha de la citada resolución (art. 19º).

La actualización del Registro es obligatoria comunicándola trimestralmente (art. 20º).

g. Derecho a indemnización por daños causados

Como se analizó previamente, la Ley 18.331 determina el principio de responsabilidad, y por lo tanto el titular es responsable de las conductas que violentan la presente ley y que generan responsabilidad administrativa, y en consecuencia de aquellas que se derivan de la responsabilidad civil y penal propiciada por los mismos hechos.

h. Derecho a la confidencialidad

Ni en la Ley 18.331 ni en el Decreto 414/009 se considera derecho, sino que se denomina principio de reserva. Exponiendo que un *derecho* es una facultad subjetiva de un titular mientras que *principio* son reglas generales de cumplimiento por parte de todos los intervinientes cuya omisión genera sanciones.

i. Derecho al olvido digital

Las características propias del derecho al olvido que lo diferencian del derecho a la supresión o cancelación, no consta en la normativa, así como tampoco ha sido desarrollado jurisprudencialmente.

j. Spam

No consta normativa específica sobre correos no deseados. Sin embargo, la Unidad Reguladora y de Control de Datos Personales del Uruguay en su informe digital "Esto es SPAM: informe sobre correo basura" señala expresamente que:

> En Aplicación de la Ley 18.331 de Protección de Datos Personales y Acción de Habeas Data en casos de SPAM En el ámbito de la protección de datos, la práctica de spam contraviene fundamentalmente el principio del previo consentimiento informado, debido a la obtención y utilización de información personal sin autorización de sus titulares, y las disposiciones relativas a la publicidad, al ignorar el ejercicio del derecho de retiro o bloqueo de sus datos.[1469]

[1469] Unidad Reguladora y de Control de Datos Personales del Uruguay, "Esto es SPAM: informe sobre correo basura", accedido 4 de septiembre de 2017, https://datospersonales.gub.uy/inicio/institucional/noticias/esto-es-spam.

De ese modo, una interpretación de la Ley 18.331 permite proteger a los uruguayos del correo basura. Por eso, se puede presentar solicitud para ser eliminados de la lista de correos, y de no ser escuchados denunciar ante la Unidad Reguladora y de Control de Datos Personales (URCDP), mediante un formulario de acceso que consta en el sitio web oficial de la citada unidad.

g) Derechos referentes a la comunicación de datos

La Ley 18.331 establece un derecho referente a la comunicación de datos, por el cual los datos personales objeto de tratamiento solo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo (art. 17). El avance de esta legislación se refiere a conceptualizar la cesión como derecho a diferencia de la mayoría de legislaciones que la toman como forma de tratamiento, o que lo contemplan dentro de las condiciones del consentimiento.

Se determina además que para la comunicación de datos, se necesita el previo consentimiento del titular que además, es revocable. No será necesario este consentimiento si existe una ley de interés general o la recabe el Estado, los datos provengan de fuentes públicas, se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento o en el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma; deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento, se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico; se incluye (por vía interpretativa) los registros y documentos destinados a la protección y contralor del trabajo (artículo 84 de la Ley N° 19355 con la cual se reforma la Ley 18.331); se trate de datos personales relativos a la salud y sea necesario por razones de salud e higiene públicas, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados; se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables. El destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor y este responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate (art. 17).

Por su parte, el Decreto 414/009 señala el derecho referente a la comunicación o la cesión de datos por parte del encargado de tratamiento, cuando resulta necesario para la prestación de un servicio al responsable, salvo que este acceso implique la existencia de un nuevo vínculo entre el encargado del tratamiento y el titular (art. 14º).

h) Derecho de actualización

Aunque la Ley 18.331 no lo menciona, el Decreto 414/009, por su parte, determina el derecho de actualización, por el cual, el titular puede modificar los datos que resulten

inexactos a la fecha de ejercicio del derecho (art. 11º). Este derecho permite materializar el principio de calidad de datos.

i) Derecho de inclusión

La Ley 18.331 no menciona el derecho de inclusión, pero el Decreto 414/009 en el artículo 12 señala que el titular tendrá derecho a incorporar una información correspondiente en una base de datos cuando acredite un interés fundado.

j) Procedimiento

Según la Ley 18.331, los titulares de los datos pueden solicitar directamente al responsable de la base de datos el acceso, la rectificación, la cancelación, la actualización y la inclusión.

El responsable de la base de datos o del tratamiento remitirá la información (art. 14) y procederá a la rectificación, actualización, inclusión o supresión, mediante las operaciones necesarias a tal fin, en un plazo máximo de cinco días hábiles de recibida la solicitud por el titular del dato o, en su caso, informar de las razones por las que estime no corresponde (art. 15).

Conforme el Decreto 414/009, los derechos de los titulares de los datos se ejercitarán por parte del titular o su representante, acreditando la identidad de ambos en su caso; se aplicará por extensión a las personas jurídicas en cuanto corresponda; en forma conjunta o independiente; exento de formalidades y en forma gratuita; mediante comunicación dirigida al responsable de la base de datos o tratamiento, que contendrá: a. Identificación del titular. b. Motivo de la solicitud. c. Domicilio real y domicilio constituido a efecto de las notificaciones. d. Fecha y firma del solicitante. e. Documentos acreditantes de la solicitud. El responsable deberá contestar la solicitud en el plazo de cinco días hábiles desde su presentación. La información que se proporcione, cualquiera sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos (art. 9º).

k) Habeas data

En el capítulo VIII, denominado "Acción de protección de datos personales", consta descrito el *habeas data*, por el cual toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicas o privadas; y –en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización– a exigir su rectificación, inclusión, supresión o lo que entienda corresponder. Cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el juez apreciará el levantamiento del mismo en atención a las circunstancias del caso (art. 37).

Vencido el plazo sin que el pedido de acceso, rectificación, actualización, inclusión o supresión sea satisfecho o si fuera denegado por razones no justificadas de acuerdo con esta ley, o el vencimiento del plazo (art. 15), quedará habilitada la acción de *habeas data* (arts. 14 y 15).

Asimismo, el titular del dato al que se deniegue total o parcialmente el ejercicio de los derechos mencionados en los incisos anteriores podrá ponerlo en conocimiento de la Unidad Reguladora y de Control de Datos Personales, quien deberá asegurarse de la procedencia o improcedencia de la denegación (art. 26).

a. Sujeto activo

La acción de habeas data podrá ser ejercida por el propio afectado titular de los datos o sus representantes, ya sean tutores o curadores y, en caso de personas fallecidas, por sus sucesores universales, en línea directa o colateral hasta el segundo grado, por sí o por medio de apoderado. En el caso de personas jurídicas, la acción deberá ser interpuesta por sus representantes legales o los apoderados designados a tales efectos (art. 39).

b. Sujetos pasivos u obligados

Todo responsable, es decir tanto el responsable de la base de datos o del tratamiento, como el encargado del tratamiento; y el tercero, sean estas personas físicas o jurídicas, públicas o privadas (art. 38).

c. Derechos tutelados por el habeas data

El derecho tutelado es la protección de datos personales que permite al titular la entrega de los datos personales o su rectificación, actualización, eliminación, inclusión o supresión (art. 38).

d. Procedencia habeas data

Procede el *habeas data* ante la negativa del responsable de la base de datos de entregar los datos personales solicitados por su titular, en las oportunidades y plazos previstos por la ley; o cuando el titular haya solicitado de la base de datos o tratamiento su rectificación, actualización, eliminación, inclusión o supresión y este no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la ley (art. 38).

e. Procedimiento del habeas data

Serán competentes para conocer las acciones de protección de datos personales o *habeas data*:

1) En la capital, los Juzgados Letrados de Primera Instancia en lo Contencioso Administrativo, cuando la acción se dirija contra una persona pública estatal, y los Juzgados Letrados de Primera Instancia en lo Civil en los restantes casos.
2) Los Juzgados Letrados de Primera Instancia del Interior a los cuales se haya asignado competencia en dichas materias (art. 38).

Las acciones se regirán por las normas propias de la Ley 18.331, así como los procesos descritos en el Código General del Procesos (art. 40).

El trámite de primera instancia determina que salvo que la acción fuera manifiestamente improcedente, en cuyo caso el tribunal la rechazará sin sustanciarla y dispondrá el

archivo de las actuaciones, se convocará a las partes a una audiencia pública dentro del plazo de tres días de la fecha de la presentación de la demanda. En dicha audiencia se oirán las explicaciones del demandado, se recibirán las pruebas y se producirán los alegatos. El tribunal, que podrá rechazar las pruebas manifiestamente impertinentes o innecesarias, presidirá la audiencia so pena de nulidad, e interrogará a los testigos y a las partes, sin perjuicio de que aquellos sean, a su vez, repreguntados por los abogados. Gozará de los más amplios poderes de policía y de dirección de la audiencia. En cualquier momento podrá ordenar diligencias para mejor proveer. La sentencia se dictará en la audiencia o a más tardar, dentro de las veinticuatro horas de su celebración. Solo en casos excepcionales podrá prorrogarse la audiencia por hasta tres días (art. 41).

Se podrán dictar medidas provisionales ante la necesidad de inmediata actuación que pretendan el amparo del derecho o libertad presuntamente violados (art. 42).

La sentencia que haga lugar al *habeas data* deberá contener: a) la identificación concreta de la autoridad o el particular a quien se dirija y contra cuya acción, hecho u omisión se conceda el *habeas data*; b) la determinación precisa de lo que deba o no deba hacerse y el plazo por el cual dicha resolución regirá, si es que corresponde fijarlo; c) el plazo para el cumplimiento de lo dispuesto, que será fijado por el tribunal conforme las circunstancias de cada caso, y no será mayor de quince días corridos e ininterrumpidos, computados a partir de la notificación (art. 43).

Acerca del recurso de apelación y segunda instancia, se determina que en el proceso de *habeas data* solo serán apelables la sentencia definitiva y la que rechaza la acción por ser manifiestamente improcedente. El recurso de apelación deberá interponerse en escrito fundado, dentro del plazo perentorio de tres días. El tribunal elevará sin más trámite los autos al superior cuando hubiere desestimado la acción por improcedencia manifiesta, y lo sustanciará con un traslado a la contraparte, por tres días perentorios, cuando la sentencia apelada fuese la definitiva. El tribunal de alzada resolverá en acuerdo, dentro de los cuatro días siguientes a la recepción de los autos. La interposición del recurso no suspenderá las medidas de amparo decretadas, las cuales serán cumplidas inmediatamente después de notificada la sentencia, sin necesidad de tener que esperar el transcurso del plazo para su impugnación (art. 44).

Para asegurar la sumariedad del proceso de *habeas data*, se prevé que en los procesos no puedan deducirse cuestiones previas, reconvenciones ni incidentes. El tribunal, a petición de parte o de oficio, subsanará los vicios del procedimiento, asegurando, dentro de la naturaleza sumaria del proceso, la vigencia del principio contradictorio (art. 45).

l) Institucionalidad de protección

La Ley 18.331 crea como órgano de control desconcentrado a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) en la cual existe la Unidad Reguladora y de Control de Datos Personales, que está dotada de la más amplia autonomía técnica (art. 31).

La Unidad Reguladora y de Control de Datos Personales[1470] deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley; asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente ley y de los medios legales de que disponen para la defensa de los derechos que esta garantiza; dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley; realizar un censo de las bases de datos alcanzados por la ley y mantener el registro permanente de los mismos; controlar la observancia de las normas sobre integridad, veracidad y seguridad de datos por parte de los responsables de las bases de datos, pudiendo a tales efectos realizar las actuaciones de inspección pertinentes; solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados; emitir opinión toda vez que le sea requerida por las autoridades competentes; informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables, en forma gratuita, entre otras (art. 34).

Finalmente, deberá asegurarse de la procedencia o improcedencia de la denegación (art. 26).

Estará dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo; a excepción del Director Ejecutivo de la AGESIC, los miembros durarán cuatro años en sus cargos, pudiendo ser designados nuevamente. Solo cesarán por la expiración de su mandato y designación de sus sucesores, o por su remoción dispuesta por el Poder Ejecutivo en los casos de ineptitud, omisión o delito, conforme a las garantías del debido proceso. Durante su mandato no recibirán órdenes ni instrucciones en el plano técnico.

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales funcionará asistido por un Consejo Consultivo, que estará integrado por cinco miembros (art. 32).

m) Régimen sancionador

La Unidad Reguladora y de Control de Datos Personales tendrá potestades sancionatorias, por las cuales el órgano de control podrá aplicar las siguientes medidas a los responsables de las bases de datos o encargados del tratamiento de datos personales en caso de que se violen las normas de la presente ley: a) apercibimiento; b) multa de hasta quinientas mil unidades indexadas; c) suspensión de la base de datos respectiva. A tal efecto, se faculta a la AGESIC a promover ante los órganos jurisdiccionales competentes, la suspensión de las bases de datos, hasta por un lapso de seis días hábiles, respecto de los cuales se comprobare que infringieren o transgredieren la presente ley.

Los hechos constitutivos de la infracción serán documentados de acuerdo con las formalidades legales, y la suspensión deberá decretarse dentro de los tres días siguientes a aquel en que la hubiere solicitado la AGESIC, la cual quedará habilitada a disponer

[1470] "Unidad Reguladora y de Control de Datos Personales", Sitio web institucional de la Unidad Reguladora y de Control de Datos Personales, accedido 1 de octubre de 2017, https://www.datospersonales.gub.uy/.

por sí la suspensión si el juez no se pronunciare dentro de dicho término. En este último caso, si el juez denegare posteriormente la suspensión, esta deberá levantarse de inmediato por la AGESIC. Los recursos que se interpongan contra la resolución judicial que hiciere lugar a la suspensión, no tendrán efecto suspensivo. Para hacer cumplir dicha resolución, la AGESIC podrá requerir el auxilio de la fuerza pública. La competencia de los Tribunales actuantes se determinará por las normas de la Ley Orgánica de la Judicatura, 15.750, 24 de junio de 1985, sus modificativas y concordantes (art. 35).

n) Transferencia internacional de datos

El Decreto 414/009 determina en el artículo 4, relativo a las definiciones aplicables a la materia, el concepto de transferencia internacional de datos, por el cual constituye el tratamiento de datos que supone una transmisión de estos fuera del territorio nacional, constituyendo una cesión o comunicación, y teniendo por objeto la realización de un tratamiento por cuenta del responsable de la base de datos o tratamiento establecido en territorio uruguayo.

Por su parte, la Ley 18.331 señala que se prohíbe la transferencia de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados según los estándares del Derecho Internacional o Regional en la materia (art. 23).

Sin embargo, esta prohibición no regirá cuando se trate de: a) cooperación judicial internacional; b) intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado por razones de salud o higiene públicas; c) transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable; d) acuerdos en el marco de tratados internacionales; e) cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico; f) cuando el interesado haya dado su consentimiento inequívocamente a la transferencia prevista; g) cuando la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado; h) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero; i) cuando la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; j) cuando la transferencia sea necesaria para la salvaguardia del interés vital del interesado; k) cuando la transferencia tenga lugar desde un registro que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para su consulta (art. 23).

Sin perjuicio de lo dispuesto en el primer inciso de este artículo, la Unidad Reguladora y de Control de Protección de Datos Personales podrá autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes respecto a la protección de la vida privada, de los derechos y libertades

fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos. Dichas garantías podrán derivarse de cláusulas contractuales apropiadas (art. 23).

El Decreto 414/009 determina que se considera exportador de datos personales a la persona física o jurídica, pública o privada, situada en territorio uruguayo que realice, conforme a lo dispuesto en el presente reglamento, una transferencia de datos de carácter personal a otro país (art. 4).

Asimismo, será importador de datos personales aquella persona física o jurídica, pública o privada, receptora de los datos de otro país, en caso de transferencia internacional de estos, ya sea responsable del tratamiento, encargada del tratamiento o tercero (art. 4).

o) Códigos de conducta

La Ley 18.331 declara que las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, el cual podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia (art. 36).

a) Delegado de protección de datos

Este artículo es un añadido dispuesto por la Ley No. 19.670 que reforma la Ley 18.331 a partir del modelo europeo de protección, por el cual se incluye la figura del delegado de protección de datos personales:

En este sentido, el artículo 40 de la Ley No. 19.670 señala que:

> […] las entidades públicas, estatales o no estatales, las privadas total o parcialmente de propiedad estatal, así como las entidades privadas que traten datos sensibles como negocio principal y las que realicen el tratamiento de grandes volúmenes de datos deberán designar un delegado de protección de datos.

De esta forma, la obligación de designar delegado de protección se relaciona con aquellos responsables de tratamiento que presenten mayores riesgos de vulneración debido a la naturaleza o volumen de datos que manejan.

Además, dicha norma establece entre las funciones principales de dicho delegado las de: asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales; supervisar el cumplimiento de la normativa en su entidad; proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales; actuar como nexo entre su entidad y la Unidad Reguladora y de Control de Datos Personales.

Estas atribuciones nos dan cuenta de un delegado que si bien tiene un rol asesor y de acompañamiento también puede vigilar la actuación del responsable de tratamiento a través de su rol de supervisión.

Además, se establece la necesidad de que el delegado de protección posea condiciones necesarias para el correcto desempeño de sus funciones y sobre todo actúe con autonomía técnica. Esta última característica resulta fundamental debido a que conforme ha adoptado la normativa uruguaya, el delegado asume un rol controlador.

2.15 República Dominicana (2010)

La Constitución de República Dominicana de 2010[1471] reconoce por primer vez una norma que señala que consagra el derecho a la intimidad, al buen nombre, la propia imagen, el honor personal, respeto y la no injerencia en la vida privada, familiar, y además facultad de toda persona al acceso a la información y al conocimiento de la finalidad con la que se usen esos datos, al tenor del texto siguiente:

> Artículo 44.- Derecho a la intimidad y el honor personal. Toda persona tiene derecho a la intimidad. Se garantiza el respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo. Se reconoce el derecho al honor, al buen nombre y a la propia imagen. Toda autoridad o particular que los viole está obligado a resarcirlos o repararlos conforme a la ley. Por tanto: 1) El hogar, el domicilio y todo recinto privado de la persona son inviolables, salvo en los casos que sean ordenados, de conformidad con la ley, por autoridad judicial competente o en caso de flagrante delito; 2) Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos; 3) Se reconoce la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, digital, electrónico o de todo otro tipo. Sólo podrán ser ocupados, interceptados o registrados, por orden de una autoridad judicial competente, mediante procedimientos legales en la sustanciación de asuntos que se ventilen en la justicia y preservando el secreto de lo privado, que no guarde relación con el correspondiente proceso. Es inviolable el secreto de la comunicación telegráfica, telefónica, cablegráfica, electrónica, telemática o la establecida en otro medio, salvo las autorizaciones otorgadas por juez o autoridad competente, de conformidad con la ley; 4) El manejo, uso o tratamiento de datos e informaciones de carácter oficial que recaben las autoridades encargadas de la prevención, persecución y castigo del crimen, sólo podrán ser tratados o comunicados a los registros públicos, a partir de que haya intervenido una apertura a juicio, de conformidad con la ley.[1472]

Asimismo, por esta primera ocasión, mediante el contenido del artículo 70 de la Constitución de República Dominicana se reconoce por primera vez la acción judicial de *habeas data*, por la cual toda persona tiene derecho "a conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación,

[1471] Asamblea Nacional de República Dominicana, "Constitución de Republica Dominicana de 2010", *Political Database of the Americas*, accedido 28 de enero de 2018, http://pdba.georgetown.edu/Constitutions/DomRep/vigente.html.
[1472] Ibíd.

actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística"[1473].

Esta acción es desarrollada en la Ley 137-11 Orgánica del Tribunal Constitucional y de los procedimientos constitucionales. G. O. 10622, 15 de junio de 2011,[1474] que en el texto pertinente textualmente dice:

> Artículo 64. Hábeas Data. Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme la ley. No podrá afectarse el secreto de las fuentes de información periodística. La acción de hábeas data se rige por el régimen procesal común del amparo.

Adicionalmente, consta en la Ley General de Libre Acceso a la Información Pública 200-04[1475] que consagra el derecho de información que comprende el derecho de acceder a las informaciones contenidas en actas y expedientes de la administración pública.

Por su parte, la Ley 172-13 tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. G. O. 10737, 15 de diciembre de 2013.[1476]

a) Ámbito: Registros o ficheros públicos y privados

Según el artículo 44 de la Constitución de República Dominicana, acerca del derecho de toda persona de acceder a su información y datos sobre ella o sus bienes, hace alusión expresa a que estos consten o reposen en registros oficiales o privados, de tal manera que se incluye en el ámbito de protección tanto al público como al privado.

En el mismo sentido, la Ley 172-13, tanto en su artículo 1 como en el 2, determina que el objeto de la ley es la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, así como garantizar que no se lesione el derecho al honor y a la intimidad de las personas, y también facilitar el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 44 de la Constitución de la República Dominicana.

[1473] Ibíd.

[1474] Congreso Nacional de República Dominicana, "Ley No. 137-11 Orgánica del Tribunal Constitucional y de los procedimientos constitucionales. G. O. No. 10622 del 15 de junio de 2011", *Tribunal Constitucional de República Dominicana*, accedido 14 de febrero de 2018, https://www.tribunalconstitucional.gob.do/transparencia/base-legal-de-la-instituci%C3%B3n/ley-no-137-11/.

[1475] "Ley-No.-200-04-Libre-Acceso-a-la-Informacion-P--blica.pdf".

[1476] Congreso Nacional de República Dominicana, "Ley No. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes sean estos públicos o privados, de 13 de diciembre de 2013", *vLex*, accedido 28 de enero de 2018, https://do.vlex.com/vid/personales-archivos-bancos-cnicos-informes-516279706.

b) Naturaleza del dato

El artículo 44 de la Constitución de República Dominicana al describir el derecho de protección de datos personales establece como criterio el tratamiento de datos e informaciones personales o sus bienes; así, se colige que se usa información y datos como sinónimos, además se dimensiona el carácter personal del dato, así como la expresa mención a la información relativa a los bienes de un titular.

Por su parte, el artículo 2 de la Ley 172-13, al describir el alcance de la norma determina que es de aplicación a los datos de carácter personal registrados en cualquier banco de datos que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos en los ámbitos público y privado. Se entenderá por archivo, registro, ficheros, base o banco de datos, indistintamente, al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso. Incluye también el conjunto de informaciones que proporcionan directamente los aportantes de datos, así como otras informaciones de carácter y dominio público, ya sea por su procedencia o por su naturaleza, al tenor del artículo 6 de la ley en mención. Sobre las fuentes accesibles al público, serán aquellos archivos de datos personales cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa. Tienen la consideración de fuentes de acceso público los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, boletines oficiales y los medios de comunicación.

Sin embargo, al tenor del artículo 4 de la ley citada, se establecen restricciones al régimen de protección cuando se refiera a: 1) archivos de datos personales mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas; 2) archivos de datos personales establecidos por los organismos de investigación y de inteligencia de la República Dominicana encargados de la prevención, persecución y castigo de los crímenes y delitos; 3) archivos de datos personales referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los archivos de datos personales o tratamientos que contengan datos de este con la finalidad de notificar el fallecimiento, aportando acreditación suficiente del mismo; 4) tratamientos de datos referidos a personas jurídicas, ni a los archivos de datos personales que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquellas, consistentes en sus nombres y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

El artículo 6, relativo a las definiciones determina el de *archivo de datos personales*, como el conjunto organizado de datos de carácter personal, que sean objeto de tratamiento o procesamiento, automatizado o no, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Los mismos serán de titularidad privada o pública.

Respecto de la clasificación de los datos, el mismo artículo 6 determina los siguientes: a) *datos especialmente protegidos o datos sensibles*, que son aquellos de carácter personal que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual; b) *datos de carácter personal*, cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables, anotándose que se entiende por persona identificable, toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social; c) *datos de carácter personal relacionados con la salud*: cualquier información concerniente a la salud pasada, presente y futura, física o mental, de un individuo; d) *datos informáticos*: los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado; d) *información crediticia*: información de carácter económico, financiero, bancario o comercial relacionada a un consumidor sobre sus obligaciones, historial de pago, garantías y clasificación de deudor, de tal modo que permita la correcta e inequívoca identificación, localización y descripción del nivel de endeudamiento del titular en un determinado momento; e) *información pública:* todo registro, archivo o cualquier dato que se recopile, mantenga, procese o se encuentre en poder de las entidades públicas a las que se refiere esta ley. Asimismo, toda información que en virtud de la Constitución de la República Dominicana garantice el principio de publicidad de los actos de los Poderes del Estado y el derecho de acceso a la información pública, establecido en la Ley General de Libre Acceso a la Información Pública 200-04, 28 de julio de 2004.

Finalmente, respecto de disociación se establece esta técnica por la cual, en el tratamiento de datos personales, no pueda asociarse a persona determinada o determinable, mediante el uso de técnicas de codificación, de modo que no permita identificar a la persona física ante terceros.

c) Sujeto activo

Los sujetos activos serán todas las personas titulares de información o de datos personales o de sus bienes. No son titulares las personas jurídicas ni las personas fallecidas al tenor de lo señalado en el artículo 4 de la ley antes referida.

El artículo 6, relativo a las definiciones, determina que a efectos de la ley y su aplicación, se asumen entre los siguientes conceptos el de *afectado* o *interesado*, que se refiere a toda persona física cuyas informaciones sean objeto del tratamiento de datos, así como todo acreedor, sea este una persona física o jurídica, que tiene o ha tenido una relación comercial o de tipo contractual con una persona física para el intercambio de bienes y servicios, en la cual la persona física es deudora del acreedor. Toda información que se derive de dicha relación estará asociada por separado, tanto al deudor como al acreedor y se regirá por esta definición. Toda persona física o jurídica que haya tenido, tenga o solicite tener un bien o servicio de carácter económico, financiero, bancario, comercial, industrial, o de cualquier otra naturaleza, con una institución de intermediación financiera o con un agente económico, según proceda conforme a la ley.

El citado artículo 6 determina en el numeral 48 que se entenderá por *titular de los datos, deudor, consumidor, cliente o titular de la información* a toda persona física cuyas

informaciones sean objeto del tratamiento de datos, así como todo acreedor, sea este una persona física o jurídica, que tiene o ha tenido una relación comercial o de tipo contractual con una persona física para el intercambio de bienes y servicios, en la cual la persona física es deudora del acreedor. Toda información que se derive de dicha relación estará asociada por separado tanto al deudor como al acreedor y se regirá por esta definición. Toda persona física o jurídica que haya tenido, tenga o solicite tener un bien o servicio de carácter económico, financiero, bancario, comercial, industrial, o de cualquier otra naturaleza, con una institución de intermediación financiera o con un agente económico, según proceda conforme a la ley.

Los artículos 71 y 72 establecen régimen especial para tratamientos con fines de publicidad y de prospección comercial y aquellos relativos a encuestas, por cuanto en la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios o que permitan establecer hábitos de consumo, cuando estos figuren en documentos accesibles al público o que hayan sido facilitados por los propios titulares de los datos u obtenidos con su consentimiento. En los supuestos contemplados en el presente artículo, el titular de los datos ejercerá el derecho de acceso sin cargo alguno. El titular de los datos solicitará, en cualquier momento, el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo.

d) Sujeto pasivo

El artículo 6 de la Ley 172-13 determina que *usuario de datos, suscriptor o afiliado* es toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o mediante conexión con los mismos. Igualmente, las entidades de intermediación financiera, los agentes económicos, las entidades públicas, y las demás personas físicas o jurídicas que mantengan acuerdos con las Sociedades de Información Crediticia (SIC) para acceder a las informaciones de los consumidores.

Acerca de *responsable del tratamiento*, se entenderá que es toda persona, pública o privada, titular del archivo de datos personales que decide la finalidad, el contenido, los medios del tratamiento y el uso de la información obtenida con el tratamiento de los datos personales.

Asimismo, por *responsable de archivo, registro, base o banco de datos*, se entiende a toda persona física o jurídica, pública o privada, que es titular de un archivo, registro, base o banco de datos.

Respecto de *tercero*, es la persona física o jurídica, pública o privada, u órgano administrativo distinto del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento.

Por *destinatario o cesionario*, aquella persona física o jurídica, pública o privada, u órgano administrativo, al que se revelen los datos.

Por *encargado del tratamiento*, la persona física o jurídica, pública o privada, que realice el tratamiento de los datos personales por cuenta del responsable del tratamiento.

Por *exportador de datos personales*, la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio dominicano que realice, conforme a lo dispuesto en esta ley, una transferencia de datos de carácter personal a un país tercero.

Por *importador de datos personales*, persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos, en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

Por *agentes económicos*, personas físicas o jurídicas, proveedoras de bienes y servicios.

Por *aportantes de datos*, las instituciones de intermediación financiera, los agentes económicos y las entidades públicas que suministran información relativa a sus operaciones a una Sociedad de Información Crediticia (SIC), destinada a conformar su base de datos.

Por *cedente*, entidad que cede o transfiere información.

Por *entidades de intermediación financiera*, aquellas entidades públicas o privadas que realicen intermediación financiera con autorización previa de la Junta Monetaria.

Por *entidades públicas*, al Poder Legislativo del Estado, compuesto por el Congreso Nacional y cualquiera de sus dependencias; el Poder Ejecutivo del Estado y todas las dependencias y entidades de la administración pública; el Poder Judicial del Estado y todos sus órganos; los tribunales administrativos estatales; los ayuntamientos municipales, organismos gubernamentales u oficiales descentralizados y con autonomía pública, y las demás entidades a las que la Constitución y las leyes estatales reconozcan como de interés público.

Finalmente, se entenderá por *archivo de datos personales*, al conjunto organizado de datos de carácter personal, sean de titularidad privada o pública.

Y a continuación, determina que *archivos de datos de titularidad privada* son aquellos de los que son responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los archivos de los que sean responsables las corporaciones de derecho público.

Finalmente, el concepto de *archivos de datos de titularidad pública*, que son aquellos archivos de datos personales de los que sean responsables los órganos de la administración pública, así como las entidades u organismos vinculados o dependientes de la misma y las entidades autónomas y descentralizadas del Estado.

Por su parte, los responsables del tratamiento de datos deberán cumplir los siguientes deberes: 1) Garantizar al titular de los datos, en cualquier circunstancia, el pleno y efectivo ejercicio del derecho de hábeas data. 2) Conservar la información bajo las

condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta y uso o acceso no autorizado. 3) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley. 4) Tramitar las consultas y los reclamos formulados por los titulares de los datos. 5) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley, y, en especial, para la atención de consultas y reclamos por parte de los titulares de la información. 6) Permitir el acceso a la información únicamente a las personas que pueden tener derecho a ella, según el artículo 13 de la citada ley.

e) Objeto o bien jurídico

a. Derecho de información

Según el artículo 5, numeral 3, de la Ley 172-13, consta descrito como principio el derecho a la información, por el cual cuando se recaben datos personales que requieran del consentimiento del titular de los datos, para que se les pueda dar el tratamiento de datos o ser cedidos después de obtener dicho consentimiento, se deberá informar previamente, a por lo menos uno de los titulares de los datos, en forma expresa y clara, explicando: a) La finalidad para la que serán destinados y quiénes pueden ser sus destinatarios o clase de destinatarios. b) La existencia del archivo, registro, banco de datos o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable. c) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

b. Autodeterminación informativa

La normativa constitucional y legal no hacen referencia expresa a la autodeterminación informativa como derecho fundamental; por el contrario tanto el artículo 44 de la Constitución como el artículo 1 de la Ley 172-13 señalan que la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, provienen en garantía de los derechos a la intimidad y el honor a la persona, al respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo, así como al derecho al honor, al buen nombre y a la propia imagen.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

No existe mención expresa a este mandato, aunque el artículo 5 de la Ley 172-13 recoge el principio de licitud por el cual los archivos de datos personales no pueden tener finalidades contrarias a las leyes o al orden público, siendo debidamente registrados y apegados a los principios establecidos en esta ley.

Ahora bien, el artículo 27 de la citada norma señala que las excepciones al consentimiento para el tratamiento y la cesión de datos serán las siguientes:

> 1. Se obtengan de fuentes de acceso público; 2. Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; 3. Se trate de listas para fines mercadológicos, cuyos datos se limiten a nombre, cédula de identidad y electoral, pasaporte, identificación tributaria y demás informaciones biográficas; 4. Se deriven de una relación comercial, laboral o contractual, científica o profesional con la persona física, y resulten necesarios para su desarrollo o

cumplimiento; 5. Se trate de datos personales que reciban de sus clientes en relación a las operaciones que realicen las entidades de intermediación financiera reguladas por la Ley Monetaria y Financiera y de agentes económicos, de las Sociedades de Información Crediticia (SIC), y de las entidades que desarrollan herramientas de puntajes de crédito para la evaluación del riesgo de los deudores del sistema financiero y comercial nacional, de acuerdo a las condiciones establecidas en el artículo 5, numeral 4. Las que disponga una ley; 7. Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; 8. Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve el secreto de la identidad de los titulares de los datos mediante mecanismos de disociación adecuados; 9. Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.

f) Principios

i. Deber de información

Según el artículo 5 de la Ley 172-13 consta entre los principios el derecho de información descrito anteriormente, sin que haya mención al deber de información por parte del responsable de la base de datos. Es decir, no consta como deber sino como derecho y señala que cuando se recaben datos personales que requieran del consentimiento del titular de los datos, para que se les pueda dar el tratamiento de datos o ser cedidos después de obtener dicho consentimiento, se deberá informar previamente a por lo menos uno de los titulares de los datos, en forma expresa y clara, explicando: a) La finalidad para la que serán destinados y quiénes pueden ser sus destinatarios o clase de destinatarios. b) La existencia del archivo, registro, banco de datos o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable. c) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos (art. 5, núm. 3).

ii. Pertinencia

Este contenido está desarrollado en el principio de calidad de datos.

iii. Calidad

El artículo 5, numeral 2, de la Ley 172-13 recoge el principio de calidad de los datos, por el cual: a) Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados y pertinentes en relación al ámbito y finalidad para los que se hubieren obtenido; b) Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario; c) Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o, en su caso, completados por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate.

iv. Finalidad

El artículo 5, numeral 8, de la Ley 172-13 recoge el principio de finalidad de los datos, mediante el cual se faculta recoger datos personales para su tratamiento, cuando sean

adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para los que se hayan obtenido.

v. Seguridad

El artículo 5, numeral 5, de la Ley 172-13 señala que el principio de seguridad de los datos establece que el responsable del archivo de datos personales y, en su caso, el encargado del tratamiento, deberán adoptar e implementar las medidas de índole técnica, organizativa y de seguridad necesarias para salvaguardar los datos de carácter personal y eviten su alteración, pérdida, tratamiento, consulta o acceso no autorizado. En consecuencia: a) Queda prohibido registrar datos personales en archivos, registros o bancos de datos que no reúnan condiciones técnicas de integridad y seguridad. b) Los aportantes de datos, las Sociedades de Información Crediticia (SIC) y los usuarios o suscriptores deben adoptar las medidas y controles técnicos necesarios para evitar la alteración, pérdida, tratamiento o acceso no autorizado de los datos sobre historial de crédito que manejen o reposen en la base de datos de las SIC. c) Las SIC deben adoptar medidas apropiadas para proteger sus bases de datos contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informáticos.

vi. Consentimiento

El artículo 5, numeral 4, determina al consentimiento del afectado como uno de los principios de la ley, por el cual el tratamiento y la cesión de datos personales es ilícito cuando el titular de los datos no hubiere prestado su consentimiento previo e informado (derecho de información), libre, expreso y consciente, que deberá constar por escrito o por otro medio que permita que se le equipare, de acuerdo con las circunstancias.

Están exentos del requisito de consentimiento: los organismos de investigación y de inteligencia del Estado encargados de la prevención, persecución y castigo de los crímenes y delitos, con autorización previa de la autoridad judicial competente.

Acerca de las entidades de intermediación financiera, los agentes económicos y las demás personas físicas o jurídicas que hayan contratado los servicios de información con las Sociedades de Información Crediticia (SIC), antes de solicitar y obtener un reporte de crédito, deberán recabar del titular de los datos el consentimiento expreso y por escrito. Los usuarios o suscriptores deberán guardar absoluta confidencialidad respecto al contenido de los reportes de crédito.

Por su parte, el artículo 27 de la citada ley establece excepciones al requerimiento de consentimiento para el tratamiento y la cesión de datos cuando estos son: que la información se obtengan de fuentes de acceso público, se recaben para el ejercicio de funciones propias de los poderes del Estado o se realice entre dependencias del Estado en forma directa sobre sus respectivas competencias, incluidos los relativos a salud por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve el secreto de la identidad de los titulares de los datos mediante mecanismos de disociación adecuados o en virtud de una obligación legal, se trate de listas para fines mercadológicos, cuyos datos se limiten a nombre, cédula de identidad y electoral, pasaporte, identificación tributaria y demás

informaciones biográficas; se deriven de una relación comercial, laboral o contractual, científica o profesional con la persona física, y resulten necesarios para su desarrollo o cumplimiento; se trate de datos personales que reciban de sus clientes en relación a las operaciones que realicen las entidades de intermediación financiera reguladas por la Ley Monetaria y Financiera y de agentes económicos, de las Sociedades de Información Crediticia (SIC), y de las entidades que desarrollan herramientas de puntajes de crédito para la evaluación del riesgo de los deudores del sistema financiero y comercial nacional.

Finalmente, conforme el artículo 28, la cesión de datos personales objeto de tratamiento de datos solo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario, con el consentimiento previo de por lo menos uno de los titulares de los datos.

vii. Lealtad

El artículo 5 de la Ley 172-13 describe otro principio directamente relacionado que es el de lealtad, por el cual se impone la prohibición de recoger los datos por medios fraudulentos, desleales o ilícitos.

g) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

a. Derecho de acceso

El derecho de acceso se encuentra descrito en el artículo 44 de la Constitución de República Dominicana y es desarrollado por el artículo 10 de la Ley 172-13, por el cual determina que el derecho de acceso lo tiene toda persona, previa acreditación de su identidad, para acceder a la información y a los datos que sobre ella o sus bienes reposen en bancos de datos públicos, en los registros oficiales de las entidades, organismos y empresas públicas, así como sus datos registrados en los archivos de las instituciones y las empresas privadas, o en los bancos de datos privados. El usuario del banco de datos debe proporcionar la información solicitada por el titular de los datos dentro de cinco (5) días hábiles posteriores a haber sido hecha de manera personal dicha solicitud, o vía acto de alguacil. Vencido el plazo sin que se satisfaga el pedido, el titular de los datos podrá incoar una acción judicial ante un juzgado de primera instancia para conocer de la existencia y acceder a los datos que de él consten en registros o bancos de datos públicos o privados, conforme al procedimiento previsto en esta ley.

Existe una confusión, pues el artículo 7 de la Ley 172-13 establece que el derecho de consulta para la protección de datos, por el cual toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de discriminación, inexactitud o error, exigir la suspensión, rectificación y la actualización de aquellos, conforme a esta ley. Esta acción judicial se refiere directamente al derecho de acceso.

El artículo 5, numeral 2, literal d) de la Ley 172-13 determina que los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

Por su parte, el artículo 8 de la citada ley señala las condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos los datos personales de los que sea titular y que estén incluidos en un banco de datos.

El artículo 9 de la citada Ley señala la Independencia de los derechos de acceso, rectificación, cancelación y oposición, es decir que estos son derechos independientes. No puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

b. Derecho de rectificación

El artículo 14 de la Ley 172-13 determina que toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos los datos personales de los que sea titular y que estén incluidos en un banco de datos.

Por su parte, el artículo 26 señala las excepciones a los derechos de acceso, rectificación, cancelación y oposición, cuando mediante resolución judicial los responsables o usuarios de bancos de datos oficiales pueden denegar el acceso, rectificación o la supresión en función de la protección de la seguridad nacional, del orden y la seguridad pública, o de la protección de los derechos e intereses de terceros, o cuando se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de crímenes y delitos por la autoridad competente y la verificación de infracciones administrativas.

Cabe señalar el régimen especial de los datos públicos, por el cual el artículo 37 determina que la creación, modificación o supresión de los archivos de datos personales de la administración pública solo puede hacerse por medio de las disposiciones contenidas en la Ley de Función Pública, y por medio de la Ley General de Libre Acceso a la Información Pública.

c. Derecho de oposición

No consta en la normativa constitucional ni legal referencia a este derecho, aunque consta en las rúbricas de los artículos 8 y 9 de la Ley 172-13, pero no se desarrolla su contenido.

d. Derecho de cancelación

El artículo 5 de la Ley 172-13 recoge el principio de calidad de los datos, por el cual los datos, total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o, en su caso, completados por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular de los datos establecidos en la presente ley. Es decir, la supresión, además de un derecho del titular es un deber del responsable de la base de datos.

Por su parte, el artículo 15 señala que la cancelación da lugar al bloqueo de los datos, conservándose únicamente a disposición de los poderes del Estado para la atención de las posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de estas. Cumplido el citado plazo deberá procederse a la supresión. En todo caso, la supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

No consta en la normativa constitucional ni legal referencia a este derecho.

f. Derecho de consulta al registro general de protección de datos personales

No consta en la normativa constitucional ni legal referencia a este derecho.

g. Derecho a indemnización por daños causados

El artículo 16 de la Ley 172-13 determina el derecho a indemnización por parte de los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente ley, sufran daños y perjuicios; tienen el merecimiento conforme al derecho común.

h. Derecho a la confidencialidad

Conforme el artículo 5 de la Ley 172-13 consta entre los principios el deber de secreto, por el cual el responsable del archivo de datos personales y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del archivo de datos personales o, en su caso, con el responsable del mismo, salvo que sea relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública. Atendiendo a este principio, el deber de secreto contemplará además: a) El obligado será relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la seguridad nacional o la salud pública. b) Todas las personas físicas o jurídicas, las entidades públicas o privadas, debidamente reconocidas como usuarios o suscriptores de una Sociedad de Información Crediticia (SIC), que tengan acceso a cualquier información relacionada con el historial de un titular de los datos, de conformidad con esta ley, deberán guardar la debida reserva sobre dicha información y, en consecuencia, no revelará a terceras personas, salvo que se trate de una autoridad competente. Los funcionarios públicos o empleados privados que con motivo de los cargos que desempeñen tengan acceso a la información de que trata esta ley, están obligados a guardar la debida reserva, aun cuando cesen en sus funciones. c) Fuera de los fines establecidos en esta ley, se prohíbe la divulgación, la publicación, la reproducción, la transmisión y la grabación del contenido parcial o total de un reporte de cualquier tipo proveniente de una Sociedad de Información Crediticia (SIC), referente a un titular de los datos, en cualquiera de sus manifestaciones, en cualquier medio de comunicación masivo, sea impreso, televisivo, radial o electrónico.

i. Derecho al olvido digital

No consta en la normativa constitucional ni legal específica referencia a este derecho.

j. Spam

No consta en la normativa constitucional ni legal específica referencia a este derecho.

h) Procedimiento

Para las *acciones de acceso*, el usuario del banco de datos debe proporcionar la información solicitada por el titular de los datos dentro de cinco (5) días hábiles posteriores a haber sido hecha de manera personal dicha solicitud, o vía acto de alguacil. Vencido el plazo sin que se satisfaga el pedido, el titular de los datos podrá incoar una acción judicial ante un juzgado de primera instancia para conocer de la existencia y acceder a los datos que de él consten en registros o bancos de datos públicos o privados, conforme al procedimiento previsto en esta ley, artículo 10.

Respecto de los derechos de rectificación y cancelación, conforme el artículo 8 de la Ley 172-13, el responsable del banco de datos, después de verificar y comprobar la pertinencia de la reclamación, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin, en el plazo máximo de diez (10) días hábiles de recibido el reclamo del titular de los datos o advertido el error o inexactitud. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más requisitos la acción de protección de los datos personales o de *habeas data* prevista en esta ley.

En el supuesto de cesión o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro de cinco (5) días hábiles de efectuado el tratamiento del dato.

Durante el proceso de verificación y rectificación del error o inexactitud de la información de que se trate, el responsable o usuario del banco de datos deberá consignar, al proveer información relativa al demandante, la circunstancia de que se encuentra sometida a revisión o impugnación.

La rectificación, actualización o supresión de datos personales inexactos o incompletos que existan en registros públicos o privados se efectuará sin cargo alguno para el interesado.

El artículo 11 señala el procedimiento de acceso ante la Sociedad de Información Crediticia (SIC) respecto de su historial crediticio o reporte de crédito, de forma gratuita cuatro (4) veces por año, y a intervalos no inferiores a tres (3) meses, salvo que se demuestre un interés legítimo al efecto; opcionalmente, el titular de los datos puede solicitar el acceso seguro mediante una plataforma vía Internet. Dicho reporte de crédito deberá ponerlo a disposición del titular de los datos en un plazo no mayor de cinco (5) días hábiles, según el artículo 12.

i) Habeas data

El artículo 70 de la Constitución de República Dominicana reconoce por primera vez la acción judicial de *habeas data*, por la cual toda persona tiene derecho "a conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística"[1477].

Esta consta desarrollada en la Ley 137-11 Orgánica del Tribunal Constitucional y de los procedimientos constitucionales, G. O. 10622, 15 de junio de 2011,[1478] cuyo texto pertinente textualmente dice:

> Artículo 64. Hábeas Data. Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme la ley. No podrá afectarse el secreto de las fuentes de información periodística. La acción de hábeas data se rige por el régimen procesal común del amparo.

a. Sujeto activo

Las normas constitucionales citadas establecen al sujeto activo como toda persona. El artículo 18 de la Ley 172-13 determina que la acción de protección de los datos personales o de *habeas data* será ejercida por el afectado, sus tutores, los sucesores o sus apoderados. Cuando la acción judicial sea ejercida por personas jurídicas deberá ser interpuesta por sus representantes legales o los apoderados que estas designen a tal efecto.

b. Sujetos pasivos u obligados

El artículo 19 de la Ley 172-13 dispone que la acción judicial procederá con respecto a los responsables y usuarios de bancos de datos públicos y privados destinados a proveer informes, cuando actúen contrario a las disposiciones establecidas en la presente ley.

c. Derechos tutelados por el habeas data

Conforme el artículo 17 de la Ley 172-13, los derechos tutelados por el *habeas data* son los de acceso, rectificación, supresión, cancelación o actualización.

Ahora bien, la normativa constitucional y legal vigente señala que la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, provienen en garantía de los derechos a la intimidad y el honor personal, al respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo, así como al derecho al honor, al buen nombre y a la propia imagen.

[1477] Asamblea Nacional de República Dominicana, "Constitución de Republica Dominicana de 2010".
[1478] Congreso Nacional de República Dominicana, "Ley No. 137-11 Orgánica del Tribunal Constitucional y de los procedimientos constitucionales. G. O. No. 10622 del 15 de junio de 2011".

d. Procedencia habeas data

El artículo 17 de la Ley 172-13 dispone que, sin perjuicio de los mecanismos establecidos para el ejercicio de los derechos de los interesados, estos puedan ejercer la acción judicial de *habeas data* de conformidad con la Constitución y las leyes que rigen la materia. La acción judicial de *habeas data* procederá para tomar conocimiento de la existencia de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados que se deriven de una relación comercial, laboral o contractual con una entidad pública o privada; o simplemente, para tomar conocimiento de los datos personales que se presuma que existen almacenados en archivos, registros o bancos de datos públicos o privados. En los casos en que se presuma inexactitud, la desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentre prohibido en la presente ley, para exigir su rectificación, supresión o actualización.

e. Procedimiento del habeas data

Respecto del procedimiento de *habeas data*, se establece en el artículo 20, que será competente para conocer de esta acción el juez del domicilio del demandado, y para el caso de pluralidad de demandados, en el domicilio de uno de ellos. Y el procedimiento aplicable consta descrito en el artículo que menciona que la acción de *habeas data* se tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo. El registro o el banco de datos, mientras dure el procedimiento, debe asentar o publicar en los informes que la información cuestionada está sometida a un proceso judicial o de impugnación de *habeas data*. El juez requerirá, mediante resolución motivada, al archivo, registro o banco de datos la remisión de la información concerniente al demandante. Podrá, asimismo, solicitar informes sobre el soporte técnico de datos (art. 22).

Los legitimados pasivos, al contestar el informe, el archivo, registro o banco de datos deberán expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no obtemperó al pedido efectuado por el interesado (art. 23). Podrá solicitarse ampliación de la demanda de *habeas data*, por el término de diez (10) días hábiles, en el cual el demandante deberá presentar las pruebas fehacientes de que su caso se trata de una información incorrecta, errónea o inexacta, y podrá exigir la suspensión, rectificación y actualización de aquellas informaciones que afecten ilegítimamente sus derechos (art. 24). Existe un procedimiento propio de reclamación aplicable a las Sociedades de Información Crediticia (SIC) para la modificación, rectificación y cancelación de la información del titular, cuando los titulares de los datos no estén conformes con la información contenida en un reporte. Por lo que la reclamación pertinente deberá presentarse por instancia o mediante acto de alguacil en el que se señale con claridad los registros en que conste la información impugnada, así como copias de la documentación en que fundamenten su inconformidad, y además de tramitar y contestar en debida forma, deberá incluir en el registro de que se trate la leyenda: "Registro Impugnado por Hábeas Data", la cual no se eliminará hasta que concluya el trámite contenido en el numeral anterior.

j) Institucionalidad de protección

El artículo 29 de la Ley 172-13 señala que los archivos, registros o bancos de datos, públicos o privados, destinados a proveer informes crediticios estarán sujetos a la inspección y vigilancia de la Superintendencia de Bancos como órgano de control, incluso antes del inicio de actividades, las Sociedades de Información Crediticia (SIC) deberán inscribirse en el registro público de Sociedad de Información Crediticia (SIC) que estará a cargo de dicha Superintendencia (art. 34).

No consta otra autoridad de protección para las otras finalidades de los datos personales.

k) Régimen sancionador

Se establecen varios regímenes aplicables a distintos ámbitos:

Sanciones administrativas para las Sociedades de Información Crediticia. El artículo 81 establece las sanciones administrativas propias de las Sociedades de Información Crediticia (SIC) que serán establecidas por la Superintendencia de Bancos. En caso de fallo adverso a la Sociedad de Información Crediticia (SIC) ante el Tribunal Superior Administrativo, la Sociedad de Información Crediticia (SIC) dispone de un plazo de un (1) mes para recurrir en casación, de conformidad con la ley que instituye el Procedimiento de Casación. La Superintendencia de Bancos no puede ejercer las facultades estipuladas en la presente ley en perjuicio de una Sociedad de Información Crediticia (SIC) hasta tanto no intervenga una decisión definitiva y con la autoridad de la cosa irrevocablemente juzgada (art. 83).

Sanciones excepcionales. El artículo 84 señala que será sancionado con una multa de diez (10) a cincuenta (50) salarios mínimos vigentes, sin perjuicio de las reparaciones que procedan por los daños y perjuicios que haya sufrido la persona por causa de violación a su derecho a la privacidad, conforme a las normas del derecho común, la persona física que: 1. Insertara o hiciera insertar, a sabiendas, datos falsos en un archivo de datos personales, de manera dolosa o de mala fe. 2. Proporcionará, de manera dolosa o de mala fe, información falsa a un tercero, contenida en un archivo de datos personales. 3. Accediere a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, de cualquier forma, a un banco de datos personales. 4. Revelare a otra información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Sanciones civiles. El artículo 85 dispone que agotado el procedimiento de solicitud y rectificación establecido en la presente ley, se considerarán infracciones civiles: 1. Denegar, sin fundamento, una solicitud de revisión o una solicitud de rectificación de la información crediticia requerida por el titular de la información. 2. Negarse a modificar o a cancelar la información de un titular de la información, luego de que este haya obtenido un pronunciamiento favorable en un procedimiento seguido de conformidad con lo establecido en la presente ley. 3. Infringir de manera grave o reiterada las disposiciones de las sentencias de los tribunales civiles con la autoridad de la cosa irrevocablemente juzgada.

Sanciones penales. El artículo 86 señala que en caso de que un usuario o suscriptor haya accedido a una base de datos para consultar, de manera fraudulenta, las informaciones personales de un titular sin haber obtenido de este autorización previa, será sancionado con multa que irá de diez (10) a cincuenta (50) salarios mínimos vigentes, sin perjuicio

de las reparaciones que procedan por los daños y perjuicios que haya sufrido la persona por causa de violación a su derecho a la privacidad, conforme a las normas del derecho común. Al usuario o suscriptor o cualquier persona física que utilice o facilite un reporte de crédito, con la finalidad de la comisión de un delito, se impondrá una sanción equivalente a prisión correccional de seis meses a dos años. Se considerará una circunstancia agravante del crimen imputado el hecho de que un usuario o suscriptor haga uso de un reporte de crédito, con la finalidad de la comisión de un crimen.

Por su parte, el artículo 87 señala que una persona física haya accesado de manera fraudulenta la base de datos para obtener y utilizar cualquier tipo de reporte proveniente de una Sociedad de Información Crediticia (SIC), utilizando claves de acceso que no le pertenecen, será sancionada con multa que irá de veinte (20) a cien (100) salarios mínimos vigentes, sin perjuicio de las reparaciones que procedan por los daños y perjuicios que haya sufrido la persona por causa de violación a su derecho a la privacidad, conforme a las normas del derecho común. En el caso de que el uso indebido de dicho reporte haya tenido como finalidad la comisión de un delito, se impondrá a la persona física que haya accesado fraudulentamente el reporte y a quien lo utilice o se prevalezca de este, una sanción equivalente a prisión correccional de seis meses a dos años; y en caso de que haya tenido como finalidad la comisión de un crimen, será sancionado con la prisión que establezca el Código Penal vigente.

l) Transferencia internacional de datos

El artículo 80 de la ley analizada señala que la transferencia internacional de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que requieran del consentimiento del titular solo se efectuarán si: 1. La persona física, libre y conscientemente, decidiera autorizar por voluntad propia la transferencia de datos, o cuando las leyes lo permitan. 2. Se trate de intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado o una investigación epidemiológica, o por razones de salud o higiene pública. 3. Se trate de transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable. 4. La transferencia de datos se hubiera acordado o contemplado en el marco de tratados internacionales o convenios, y en los tratados de libre comercio de los cuales sea parte la República Dominicana. 5. La transferencia de datos tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, la trata de personas, el narcotráfico, y demás crímenes y delitos. 6. La transferencia de datos sea necesaria para la ejecución de un contrato entre el titular de los datos y el responsable del tratamiento, o para la ejecución de medidas precontractuales. 7. La transferencia de datos legalmente exigida sea para la salvaguarda del interés público o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, o solicitada por una administración fiscal o aduanera para el cumplimiento de sus competencias. 8. La transferencia de datos se efectúe para prestar o solicitar un auxilio judicial internacional. 9. La transferencia de datos se efectúe a petición de un organismo internacional con interés legítimo desde un registro público.

Por su parte, el artículo 89 señala que todo lo relacionado con la protección de las personas físicas, en lo que respecta al tratamiento de datos de carácter personal, en relación a cualquier convenio o tratado internacional del que sea signataria la República Dominicana, se regirá conforme a sus disposiciones.

m) Códigos tipo

Los artículos 73 y 74 establecen que mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, pueden formular códigos tipo que establezcan las condiciones detalladas de cada sistema particular y estándares técnicos de aplicación, organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente ley.

2.16 Costa Rica (2011)

Constitución Política de la República de Costa Rica de 1949, con Reformas de 1954, 1956, 1957, 1958, 1959, 1961, 1963, 1965, 1968, 1969, 1971, 1975, 1977, 1981, 1982, 1984, 1987, 1989, 1993, 1994, 1995, 1996, 1997, 1999, 2000, 2001, 2002 y 2003 (Ley 8365, 15 de julio del 2003).[1479]

La Constitución costarricense no reconoce expresamente el derecho a la protección de datos personales, únicamente se consagra el derecho a la intimidad y su directo relacionamiento con la inviolabilidad de las comunicaciones, de la correspondencia y documentos privados, tal como se describe en el artículo 24 que se transcribe a continuación:

> Artículo 24.- Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones. Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá de los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento. Igualmente, la ley determinará en cuales casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas, podrán ejecutarse de inmediato. Su aplicación y control, serán responsabilidad indelegable, de la autoridad judicial. La ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos. Una ley especial, aprobada por dos tercios del total de los Diputados, determinará cuales otros órganos de la Administración Pública podrán revisar los documentos que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión. No producirán efectos legales, la correspondencia que fuere

[1479] Asamblea Nacional Constituyente, "Costa Rica: Constitución Política de 7 de noviembre de 1949 y sus Reformas", *Political Database of the Americas*, accedido 28 de septiembre de 2017, http://pdba.georgetown.edu/Constitutions/Costa/costa2.html.

> sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación. (Así modificado por la Ley 7607, 29 de mayo de 1996).

El reconocimiento del derecho a la protección de datos personales en Costa Rica es de origen jurisprudencial, mediante las resoluciones que por acción de amparo ha dictado la Sala Constitucional:

> [Las]... sentencias 4154-97, 7175-97, 4347-99 y 5802-99 reconocieron la existencia de un derecho a la tutela jurisdiccional privilegiada de los datos personales (habeas data), desarrollando una serie de principios atinentes al acopio, almacenamiento y empleo de bases de datos, lista que ha sido ampliada y delimitada por diversos fallos posteriores, tales como las sentencias 1345-98, 1119-00, y 00754-02, que reconocen expresamente la existencia de un derecho a la autodeterminación informativa y desarrollan en detalle sus postulados esenciales, en particular el principio de calidad de los datos y de adecuación al fin para el cual fueron obtenidos. Estas tres sentencias demuestran que la Sala Constitucional decidió entender en forma amplia la relación existente entre el derecho a la intimidad y el principio democrático, observándola como un presupuesto esencial para el ejercicio de otros derechos fundamentales previstos en la Constitución, que definen al ciudadano como una entidad que actúa libre, interactuando con otros y desarrollando su plan de vida libre de intervenciones estatales o privadas, mientras este plan no entre en contradicción con las bases del sistema. [...] Finalmente, la sentencia 08996-02 va todavía más allá y reconoce los derechos a recibir información acerca del uso que será dado a los datos suministrados, al consentimiento necesario para que tales informaciones puedan ser recogidas, almacenadas y manipuladas, y sienta algunas bases de lo que deberá en el futuro ser la regulación de la transferencia nacional e internacional de datos entre diversos ficheros. Es decir, recoge muchos de los principios modernamente entendidos como propios de una adecuada protección de datos.[1480]

Pese a este notorio avance de reconocimiento constitucional del derecho, es recién en el año 2011 cuando se dicta la normativa específica que, además de armonizar las resoluciones judiciales, desarrolla su contenido esencial:

- Ley Protección de la Persona frente al tratamiento de sus datos personales 8968, 7 de noviembre de 2011,[1481] (en adelante Ley 8968).
- Decreto Ejecutivo 37554, 30/10/2012, Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, Publicado en el Alcance Digital 42 a La Gaceta 45, 05 de marzo de 2013, reformado por el Decreto Ejecutivo 40008-JP, Costa Rica, 6 de diciembre de 2016[1482] (en adelante Decreto Ejecutivo 37554).

[1480] M. CARVAJAL PÉREZ Y A. CHIRINO SÁNCHEZ, "El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica", en José Luis Piñar Mañas, Álvaro Canales Gil, María José Blanco Antón, Mercedes Ortuño Sierra, ed., *Protección de datos de carácter personal en Iberoamérica* (Valencia: Tirant lo Blanch, 2006), 251-253.

[1481] Asamblea Legislativa de la República de Costa Rica, "Ley de Protección de la Persona frente al tratamiento de sus datos personales Nº 8968 de 7 de julio de 2011", *Sistema Costarricense de Información Jurídica*, 2011, accedido 28 de septiembre de 2017, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&param2=1&strTipM=TC&lResultado=3&strSim=simp.

[1482] Poder Ejecutivo de la República de Costa Rica, "Decreto Ejecutivo: 37554 del 30/10/2012, Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales N° 37554-JP", *Sistema Costarricense de Información Jurídica*, 2012, accedido 28 de septiembre de 2017, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74352&nValor3=106487&strTipM=TC.

- Directriz 46-H-MICITT, 09/04/2013, Las instituciones del sector público privilegiarán la adquisición de soluciones de cómputo en la nube sobre otro tipo de infraestructura.[1483]
- Reglamento 39, 11/08/2014, Reglamento de actuación de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales en el Poder Judicial (Ley 8968), 8 de octubre del 2014, dictada por la Corte Plena del Poder Judicial de la República de Costa Rica.[1484]
- Acuerdo 0, 04/04/2014, Las personas físicas o jurídicas públicas o privadas propietarias o administradoras de bases de datos deberán adecuar sus procedimientos y reglas de actuación para cumplir con la Ley 8968, Ley de Protección de la Persona frente Tratamiento Datos Personales, 4 de abril del 2014, aprobado por el Ministerio de Justicia y Paz de la República de Costa Rica.[1485]
- Ley 7135, 11/10/1989, Ley de la Jurisdicción Constitucional, Asamblea Legislativa, incluye la reforma realizada al 31/10/2011[1486] que regula el recurso de amparo con el cual se protege de transgresiones a derechos fundamentales como la intimidad.

a) Ámbito: Registros o ficheros públicos y privados

Conforme el artículo 2 de la Ley 8968, relativa al ámbito de aplicación de la ley, esta protege los datos personales que se encuentran en bases de datos automatizadas o manuales incluidas modalidades de uso posterior de datos, tanto de organismos públicos como privados, los datos contenidos en bases mantenidas por personas físicas o jurídicas con fines internos, personales o domésticos, siempre y cuando estas no sean vendidas o de cualquier otra manera comercializadas.

En el mismo sentido, el Decreto Ejecutivo 37554, reformado por el Decreto Ejecutivo 40008, 19 de julio de 2016, señala idéntico texto al constante en la ley en el artículo 3 de este reglamento, pero añade que la protección de los datos se extenderá en el

[1483] Poder Ejecutivo de la República de Costa Rica, "Directriz: 46 del 09/04/2013 Las instituciones del sector público privilegiarán la adquisición de soluciones de cómputo en la nube sobre otro tipo de infraestructura N° 46-H-MICITT", 2013, accedido 28 de septiembre de 2017, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74850&nValor3=92560&strTipM=TC.

[1484] Corte Plena del Poder Judicial de Costa Rica, "Reglamento: 39 del 11/08/2014, Reglamento de actuación de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales en el Poder Judicial (Ley N° 8968)", *Sistema Costarricense de Información Jurídica*, 2014, accedido 28 de septiembre de 2017, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=78310&nValor3=98645&param2=1&strTipM=TC&lResultado=1&strSim=simp.

[1485] Ministerio de Justicia y Paz de la República de Costa Rica, "Acuerdo 0 del 4 de abril del 2014, Las personas físicas o jurídicas públicas o privadas propietarias o administradoras de bases de datos deberán adecuar sus procedimientos y reglas de actuación para cumplir con Ley N° 8968 Protección de la Persona frente tratamiento datos personales", *Sistema Costarricense de Información Jurídica*, 2014, accedido 28 de septiembre de 2017, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=77324&nValor3=96852&param2=1&strTipM=TC&lResultado=2&strSim=simp.

[1486] Asamblea Legislativa de la República de Costa Rica, "Ley: 7135 del 11/10/1989, Ley de la Jurisdicción Constitucional", *Sistema Costarricense de Información Jurídica*, accedido 2 de octubre de 2017, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=45394&nValor3=47836&param2=1&strTipM=TC&lResultado=2&strSim=simp.

territorio nacional, o les resulte aplicable la legislación costarricense derivada de la celebración de un contrato o en los términos del derecho internacional. Añade que las bases de datos de entidades financieras que se encuentren sujetas al control y regulación por parte de la Superintendencia General de Entidades Financieras (SUGEF) no requerirán inscribirse ante la Agencia de Protección de Datos de los Habitantes, aunque podrán ser reguladas y fiscalizadas y podrá ejercerse todas las acciones de protección de los datos consagradas en la Ley 8968.

Asimismo, el reglamento determina que estarán excluidas del ámbito de la ley y del reglamento las personas físicas en su calidad de profesionales, siempre y cuando ello se realice para fines propios de la profesión o en cumplimiento de disposiciones legales.

b) Naturaleza del dato

El artículo 3 de la Ley 8968 contempla las siguientes definiciones para los efectos de la ley, empezando por la *Base de datos*, denominada así como cualquier conjunto estructurado de datos personales que requieran tratamiento o procesamiento en cualquier modalidad de su elaboración, organización o acceso. Por su parte, los *datos personales* aluden al dato relativo a una persona física, identificada o identificable, derivándose por su naturaleza en dos accesos que atienden a los nombres de *irrestricto* que hace referencia a los contenidos en bases de datos públicas y de acceso general conforme la finalidad a la que serán sometidos atendiendo a lo que dispongan leyes especiales; y *restringido*, diferenciándose del anterior mencionado por ser interés solo de su titular o para la Administración Pública. En el mismo sentido, los *datos sensibles* se revelan como información relativa al fuero íntimo de la persona. Además, este artículo revela a su vez el *tratamiento correspondiente a los datos personales*, siendo esta cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales como a cualquier forma que facilite el acceso a estos.

Finalmente, el artículo 9 determinó las categorías particulares de los datos clasificándolos como:

a) *Datos sensibles*, que consisten en aquellos que revelan el origen racial o étnico, opiniones políticas, convicciones religiosas, espirituales o filosóficas, así como los relativos a la salud, la vida y la orientación sexual, entre otros Nadie estará obligado a suministrarlos y su tratamiento se considera prohibido, a menos que sea necesario para salvaguardar el interés vital del interesado o de otra persona cuando: a) la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento; b) se efectúe en actividades legítimas de una fundación, una asociación o cualquier otro organismo, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo, por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de las personas interesadas; c) aquellos necesarios para el ejercicio de la defensa de un derecho en un procedimiento judicial; d) para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por

un funcionario o funcionaria del área de la salud, sujeto al secreto profesional.

b) *Datos personales de acceso restringido*, aquellos que, aun formando parte de registros de acceso al público, no son de acceso libre por ser de interés solo para su titular o para la Administración Pública. Su tratamiento será permitido únicamente para fines públicos o si se cuenta con el consentimiento expreso del titular.

c) *Datos personales de acceso irrestricto*, los contenidos en bases de datos públicas de acceso general, según lo dispongan las leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados. No se considerarán contemplados en esta categoría: la dirección exacta de la residencia, excepto si su uso es producto de un mandato, citación o notificación administrativa o judicial, o bien, de una operación bancaria o financiera, la fotografía, los números de teléfono privados y otros de igual naturaleza cuyo tratamiento pueda afectar los derechos y los intereses de la persona titular.

d) *Datos referentes al comportamiento crediticio*, que son los referentes al comportamiento crediticio; se regirán por las normas que regulan el Sistema Financiero Nacional, de modo que permitan garantizar un grado de riesgo aceptable por parte de las entidades financieras, sin impedir el pleno ejercicio del derecho a la autodeterminación informativa ni exceder los límites de esta ley.

El artículo 2 del Decreto Ejecutivo 37554 expone ciertas definiciones, además de las establecidas en la ley como:

a) *Base de datos*, como cualquier conjunto estructurado de datos personales públicos o privados, objeto de tratamiento manual o automatizado, en el sitio o en la nube, cualquiera que sea la modalidad de su elaboración, organización o acceso, bajo dirección de un responsable.

b) Por otra parte, en esta sección, reformada por el Decreto Ejecutivo en el 2016 se encuentra regulado el concepto de *Base de datos interna, personal y doméstica y Base de datos interna*, ambas definidas como un conjunto estructurado de datos personales, que cumplen con la condición de que no ser comercializadas, distribuidas o difundidas en sí mismas o su contenido. Sin embargo, distan en que la primera es de acceso irrestricto y mantenida por personas físicas, a diferencia de la última que es mantenida por personas jurídicas públicas o privadas; y determina en esta consideración solo a los datos compartidos de un mismo grupo de interés económico local o internacional siempre que no medie difusión, distribución, venta o comercialización a terceros.

c) En este sentido se conceptualiza *Bases de datos de acceso púbico* como un conjunto de estructurado de datos que puede ser consultado por cualquier persona a las que no impida una norma limitativa sin más exigencia que el pago de una contraprestación.

d) Así también, *Datos en la nube*, tal como un conjunto estructurado de datos a los que se accede mediante internet y Fichero, descrito como todo conjunto de datos personales, cualquiera que fuere su creación, almacenamiento, organización y acceso.

e) Finalmente, se determina el concepto de *Procedimiento de disociación*, explicado como la acción y efecto de disociar datos personales de modo que la información obtenida no pueda asociarse a persona determinada o determinable. Este proceso se usa para la investigación científica manifestada como el proceso de aplicación de un método científico que procuran tener información relevante y fidedigna para expresarla en los datos de carácter no sensible o sensibles no identificables con el fin de obtener conocimientos y solucionar problemas científicos, filosóficos o empírico-técnicos.

   En este sentido, se exhibe a su vez el *tratamiento de datos*, tipificado como cualquier operación o conjunto de ellas efectuadas, automatizada o manualmente, y aplicadas a datos personales efectuado mediante tecnologías de la información que permitan el acceso a estos el cotejo, o la interconexión, así como su bloqueo, supresión o destrucción, intercambio o digitalización de datos personales, entre otros.

c) Sujeto activo

Según el artículo 3 de la Ley 8968, se define como *Interesado* a la persona física, titular de los datos que sean objeto de tratamiento manual o automatizado, con lo cual se excluye expresamente a la persona jurídica.

En ese mismo sentido, el Decreto Ejecutivo 37554, en el artículo 2, añade que también se considera titular o interesado, persona física dueña de los datos personales tutelados en la ley. Llama la atención la utilización del término "dueño" debido a que este se asocia a una de las condiciones del derecho de propiedad, que no es el caso, porque la protección de datos personales por tratarse de un derecho fundamental en realidad debe utilizar el término titularidad.

Finalmente, se entiende por persona física identificable aquella cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a la misma y que no se considerará así si dicha identificación requiere plazos o actividades desproporcionadas.

d) Sujeto pasivo

Con base en lo que concibe el artículo 3 de la Ley 8968, se define como *responsable de la base de datos*, a la persona física o jurídica de entidad pública o privada que administre, gerencie o se encargue de la base de datos, y con arreglo a la ley determine su finalidad, registrando el procedimiento a aplicar.

El artículo 2 del Decreto Ejecutivo 37554, además, declara la concepción de Encargado, Intermediario tecnológico o proveedor de servicios y Responsable, los tres identificados

como personas físicas o jurídicas de entidad pública o privada, distinguiéndose porque el primero da tratamiento a los datos personales por cuenta del responsable de datos; el segundo brinda servicios de infraestructura, plataforma, *software* u otros; y el último no difiere del trato que se le da en la ley anteriormente expuesta, añadiendo la categoría de propietario dentro de la cualidad de la persona.

e) Objeto o bien jurídico

a. Derecho de información

Aparece este derecho como consecuencia del deber de información constante en el artículo 5, el cual se refiere a consentimiento informado.

b. Autodeterminación informativa

En los considerandos de la Ley 8968, se determina que esta es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Por ello, el capítulo II, titulado "Principios y derechos básicos para la protección de datos personales", sección I, denominada "Principios y derechos básicos", en el artículo 4 declara que toda persona tiene derecho a la autodeterminación informativa la cual abarca principios y garantías relativas al legítimo tratamiento de su datos personales, conjuntamente; se la reconoce como un derecho fundamental y que, partiendo del derecho de privacidad, controla el flujo de información que concierne a cada persona, y evita acciones discriminatorias.

El Decreto Ejecutivo 37554, en el artículo primero, sostiene que el objeto de si es reglamentar garantizando a cualquier individuo el respeto al derecho de la autodeterminación informativa, relacionada con su intimidad o actividad privada, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

En este enfoque, el artículo 12 del mismo apartado conduce a la autodeterminación informativa, siendo este el derecho fundamental de toda persona física a conocer lo que conste sobre sí en cualquier base de datos pública o privada, el fin para el cual se da uso a su información personal, así como exigir su rectificación cuando sea incorrecta o inexacta, o no sea empleada para un fin autorizado o legítimo.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

La Ley 8968 plantea en el artículo 8 las excepciones a la autodeterminación informativa, aludiendo a los principios, derechos y garantías. En este sentido, podrán ser limitados acorde con el principio de transparencia administrativa cuando se persiga la seguridad del Estado; la seguridad y el ejercicio de la autoridad pública; la prevención, persecución, investigación, detención y represión de las infracciones penales, o de la

deontología en las profesiones; el funcionamiento de bases de datos que se manipulen con fines estadísticos, históricos o de investigación científica, siempre que no exista riesgo de identificación; la correcta prestación de servicios públicos y la eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales.

d. Principios

i. Deber de información

De acuerdo con el artículo 5 de la Ley 8968, y dentro del principio de consentimiento informado, consta la obligación de informar, cuando se soliciten datos de carácter personal a su titular o representante de modo expreso en lo relacionado con: la existencia de una base de datos personal, los fines que se persiguen con su recolección, los destinatarios y quienes podrán consultar la información, del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección, el tratamiento que se aplicará, las consecuencias de la negativa a suministrarlos, la posibilidad de ejercer derechos y la identidad y dirección de quien asume responsabilidad sobre la base de datos. Incluyendo también que, en caso de utilizar cuestionarios u otro medio de recolección de datos personales, deben figurar los mencionados puntos en forma claramente legible.

ii. Pertinencia

Puede entenderse este principio como inmerso en el de calidad de los datos personales, constante en el artículo 6 de la Ley 8968, en el momento en el que se señala que los datos deberán ser exactos cuando la persona responsable de la base de datos tomará las medidas necesarias para que los datos sean exactos y completos, con respecto a los fines para los cuales fueron recogidos o para los cuales fueron tratados posteriormente.

iii. Calidad

De acuerdo con el artículo 6 de la Ley 8968, los datos de carácter personal solo podrán ser recolectados, almacenados o empleados para su íntegro tratamiento siempre y cuando estos sean: actuales, veraces, exactos y adecuados a su finalidad. Por este motivo, el responsable de los datos deberá eliminarlos cuando no sean pertinentes o la necesidad para la cual fueron evocados ya no subsista. De la misma manera, se descartarán si afectan a su titular habiendo pasado diez años desde la fecha en que se dieron los hechos registrados. Si se prescinde su conservación, deberán ser disociados de su titular. Además, se obligará a modificar o suprimir todos aquellos datos que le falten a la verdad, sean inexactos o inconclusos y encaucen su finalidad contra la ley o la moral pública, descuidando la naturaleza de sus fines explícitos y legítimos a menos que se orienten en términos históricos, estadísticos o científicos, siempre que se ostenten de las debidas garantías que amparen los derechos.

iv. Finalidad

El principio de finalidad consta inmerso dentro del principio de calidad en la Ley 8968 cuando determina sobre la necesidad de la adecuación al fin de los datos personales; es decir que deberán ser recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines.

No se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando se establezcan las garantías oportunas para salvaguardar los derechos contemplados en esta ley.

Las bases de datos no pueden tener finalidades contrarias a las leyes ni a la moral pública.

v. Seguridad

De acuerdo con lo establecido en el artículo 10 de la Ley 8968, el responsable de la base de datos deberá adoptar las medidas necesarias para garantizar la seguridad de los datos de carácter personal y la protección de la información almacenada frente a acciones contrarias a la ley, estableciendo mecanismos de seguridad física y lógica según el desarrollo tecnológico actual. Además, no se registrarán datos personales en bases de datos que no reúnan todos los requisitos para garantizar su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas.

En ese contexto, el reglamento en el artículo 34 trata de igual manera las medidas de seguridad para el tratamiento de datos personales y los desarrolla igual que la ley añadiendo entre sus mecanismos para este fin el administrativo y entendiendo por medidas de seguridad el control o grupo de controles para proteger los datos personales. También regula acerca de que el responsable deberá velar porque el encargado de la base de datos y el intermediario tecnológico cumplan con las mencionadas medidas para protección de la información.

Posteriormente, el reglamento que consta en el Decreto Ejecutivo 37554 desarrolla los factores para determinar las medidas de seguridad; en el artículo 35 sostiene: la sensibilidad de los datos personales tratados, en los casos que la ley lo permita; el desarrollo tecnológico; las posibles consecuencias de una transgresión para los titulares de los datos; el número de titulares de datos personales; las vulnerabilidades previas ocurridas en los sistemas de tratamiento o almacenamiento; el riesgo por el valor, cuantitativo o cualitativo, que pudieran tener los datos personales y demás factores que resulten de otras leyes o regulación aplicable al responsable.

Consecutivamente, el artículo 36 de la misma región de estudio desarrolla las acciones a fin de mantener la seguridad física y lógica de los datos personales, constando así: elaborar una descripción detallada del tipo de datos personales tratados o almacenados; crear y mantener actualizado un inventario de la infraestructura tecnológica; además –reformado por Decreto Ejecutivo en el 2016– señalar el tipo de sistema, programa, método o proceso utilizado en el tratamiento o almacenamiento de los datos; igualmente, indicarse el nombre y la versión de la base de datos utilizada cuando proceda; por otro lado, identificar peligros y estimar los riesgos que podrían afectar los datos personales; establecer las medidas de seguridad aplicables a los datos personales, e identificar aquellas implementadas de manera efectiva; calcular el riesgo residual existente basado en la diferencia de las medidas de seguridad existentes y aquellas faltantes que resultan necesarias para la protección de los datos personales; elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivados del resultado del cálculo del riesgo residual; y por último, adicionado por Decreto ejecutivo en el 2016, las medidas de seguridad de las bases de datos serán consideradas

información no divulgada y serán resguardadas exclusivamente por el responsable de la base de datos. Podrán ser requeridas por la Agencia únicamente para consulta *in situ* y para la verificación de acciones ante la existencia de una denuncia expresa de terceros afectados. Para efectos de registro se notificará a la Prodhab los protocolos mínimos de seguridad con los que cuenta el responsable.

El reglamento hace constar además, en el artículo 37, que a los responsables les corresponderá actualizar las medidas de seguridad previstas cuando: se modifiquen para su progreso continuo, derivado de las revisiones a la política de seguridad del responsable; se produzcan alteraciones sustanciales que deriven en un cambio del nivel de riesgo; se modifique la plataforma tecnológica; se vulneren los sistemas de tratamiento o almacenamiento de datos personales; o exista una afectación disímil a las anteriores. Añadiendo, se concluye que en el caso de datos personales sensibles, cuando la ley lo permita, el responsable deberá revisar y actualizar las medidas de seguridad, al menos una vez al año.

Continuando en el camino de seguridad instaurado en el reglamento, el artículo 38 entabla que el responsable deberá informar al titular sobre cualquier irregularidad que recaiga acerca del tratamiento de sus datos como consecuencia de una vulnerabilidad de la seguridad, para lo cual tendrá cinco días hábiles a fin de que los titulares puedan tomar las decisiones correspondientes.

Se concluye, en materia de seguridad, con el artículo 39 del reglamento que reza la información mínima que deberá ser presentada por parte del responsable en relación con lo expuesto en el artículo anterior: la naturaleza de incidente, los datos personales comprometidos, las acciones correctivas emprendidas de forma inmediata, los medios para obtener más información al respecto.

vi. Consentimiento

Conforme a lo expuesto en el artículo 5 de la Ley 8968, quien recopile los datos deberá contar con el consentimiento previo e informado y expreso de su titular o representante expuesto de manera escrita, el cual podrá ser revocado sin efecto retroactivo; mas este no será imperioso cuando: exista orden fundamentada dictada por una autoridad competente o acuerdo adoptado por una comisión especial de la Asamblea Legislativa; también cuando se trate de datos de acceso irrestricto y los datos deban ser entregados por disposición constitucional o legal.

Para fines de desarrollo de la materia, el reglamento define en el artículo 2 el *Consentimiento del titular de los datos personales* como toda manifestación de voluntad del titular expresa, libre, inequívoca, informada y específica que se conceda para un fin determinado, mediante la cual admita el tratamiento de sus datos personales. Y añade que, si el consentimiento se otorga en el marco de un contrato para otros fines, dicho contrato deberá contar con una cláusula específica e independiente sobre consentimiento del tratamiento de datos personales, siendo este último inciso reformado por Decreto Ejecutivo en el 2016. Por otra parte, define *Contrato global* como un acuerdo de voluntades mediante el cual las partes manifiestan o expresan su consentimiento y que tiene por objeto el servicio de un conjunto de consultas realizadas por un mismo solicitante a una base de datos que sujete datos personales, mediante el tratado de una remuneración pecuniaria.

El reglamento, Decreto Ejecutivo 37554, asimismo expone de manera detallada en los artículos 4, 5 y 6 los requisitos las formalidades y la Carga de la prueba del consentimiento. Respecto al primer punto la obtención del consentimiento deberá ser: libre, específico, informado, individualizado e inequívoco, siendo este último reformado por Decreto Ejecutivo en el 2016. En este sentido, no se deberá mediar con cualquier acción que afecte la manifestación de voluntad del titular, se justificará el tratamiento mediante la exaltación de las finalidades determinadas y definidas; además el titular debe tener conocimiento anterior al tratamiento y sus consecuencias, el consentimiento es mínimo uno por cada titular y debe otorgarse mediantes conductas inequívocas de modo que pueda demostrarse de manera indubitable su otorgamiento y permita posterior consulta.

Respecto a las formalidades del consentimiento y cuando este no es necesario, el reglamento lo desarrolla tal y como en el artículo 5 de la ley, añadiendo que si se trata de consentimiento recabado en línea, el responsable deberá poner a disposición un procedimiento para el otorgamiento del consentimiento conforme a la ley, siendo este inciso reformado por Decreto Ejecutivo en el 2016. De igual manera, el documento que declara el consentimiento del titular deberá ser de fácil comprensión, gratuito y debidamente identificado. Por último, según el artículo 6, con el objetivo de demostrar la obtención del consentimiento, la carga de la prueba recaerá en el responsable de la base de datos.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

De acuerdo con los artículos 13 y 14 del reglamento, Decreto Ejecutivo 37554, el ejercicio de cualquiera de los derechos de acceso, rectificación, modificación, revocación o eliminación de los datos personales por parte del titular, no excluye la posibilidad de ejercer unos u otros; sin embargo, podrán restringirse por razones de seguridad nacional, disposiciones de orden público y salud pública o para proteger los derechos de terceras personas, mediante resolución fundamentada y motivada.

a. Derecho de acceso

El artículo 7.1 de la Ley 8968 afirma que se garantiza el derecho de toda persona al acceso de sus datos personales, rectificación o supresión de estos y a consentir la cesión de sus datos. En este margen la persona responsable de la base de datos debe efectuar lo solicitado de manera gratuita en el término de cinco días hábiles a partir de la recepción de la solicitud. Asimismo, el derecho de acceso garantiza las facultades del interesado como: obtener en intervalos razonables la confirmación o no de la existencia de datos personales en archivos o bases de datos, y en caso de existencia sean comunicados en forma precisa y entendible. Al mismo tiempo, recibir información relativa a su persona, así como el fin y uso para el que fueron recolectados los datos mediante un informe completo, claro y exento de codificaciones acompañado de los términos técnicos que se manejen. También consta ser informado por escrito sobre la totalidad del registro perteneciente al titular; sin embargo este informe no podrá revelar datos de terceros excepto cuando con ello se pretenda configurar un delito penal. Y, por último, permite tener conocimiento del sistema, programa, método o proceso utilizado en el tratamiento

de los datos. Añadiendo que, en el caso de personas fallecidas, les corresponderá el conocimiento de tal información a sus sucesores o herederos.

Para estos efectos el artículo 21 del reglamento, Decreto Ejecutivo 37554, por su parte dispone, además de lo ya establecido en la ley, que se podrá realizar las consultas de información con un intervalo mínimo de seis meses, salvo que de manera fundamentada el titular exprese al responsable los motivos por los cuales considera que se ha violentado sus derechos.

b. Derecho de rectificación

Según el artículo 7.2 de la Ley 8968, se garantiza el derecho de rectificación, actualización o eliminación sobre datos personales o sobre la garantía de confidencialidad respecto a los mismos; en el primer caso a causa de carácter incompleto o inexacto o hayan sido recolectados sin previo consentimiento de su titular o los mismos. Completando que, en el caso de personas fallecidas, les pertenecerá el conocimiento de dicha información a sus sucesores o herederos.

En frecuencia con lo mencionado, el reglamento, Decreto Ejecutivo 37554, en el artículo 23 añade la confusión como condición para su rectificación, y el artículo 24 expone los requisitos para el ejercicio de este derecho de entre lo que se detalla: indicar a qué persona se refiere, así como la corrección que se desee aplicar debidamente custodiada de la documentación que ampare su procedencia; el responsable deberá ofrecer mecanismos que faciliten el ejercicio de este derecho.

c. Derecho de oposición

En la normativa de Costa Rica no aparece el derecho de oposición. Una aproximación, con ciertas limitaciones, se considera el denominado derecho de revocación, por el cual, en cualquier tiempo se podrá revocar el consentimiento, de la misma forma en el que este fue obtenido; es decir, por parte del titular del dato o su representante y mediante manifestación expresa y por escrito, ya sea en un documento físico o electrónico, conforme el artículo 5.2 de la Ley 8968.

d. Derecho de cancelación

Es el reglamento, Decreto Ejecutivo 37554, el netamente encargado de desarrollar el derecho de cancelación, empezando por el artículo 2 en el cual define supresión o eliminación como el procedimiento en el que el responsable borra o destruye total o parcialmente de manera definitiva, los datos personales de la base de datos del titular. En este contexto, el artículo 25 desarrolla este derecho como la posibilidad del titular para solicitar la supresión o eliminación al responsable conforme lo fundamentado en el artículo 2. Sin embargo, el artículo 26 expresa las excepciones para efectivizar el ejercicio de este derecho de entre las que constan: la seguridad del Estado; los datos deban ser mantenidos por disposición constitucional, legal o resolución de órgano judicial; la seguridad ciudadana y el ejercicio de la autoridad pública; la prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones de la deontología en las profesiones; el funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o científicos, cuando no exista riesgo de que las personas sean identificadas; la adecuada prestación de servicios públicos; la

eficaz actividad ordinaria de la Administración; se trate de datos personales de acceso irrestricto.

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

Tanto en la normativa legal como en la reglamentaria se considera el tratamiento de datos automatizados. Es decir, forma parte del ámbito de aplicación de la norma por el cual le serán aplicables todos los principios y derechos estudiados.

Asimismo, el Reglamento, Decreto Ejecutivo 37554, define a los datos por el cual cualquier operación, conjunto de operaciones o procedimientos, aplicados a datos personales, efectuados mediante la utilización de *hardware, software*, redes, servicios, aplicaciones, en el sitio o en la nube, o cualquier otra tecnología de la información que permitan la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión, distribución o cualquier otra forma que facilite el acceso a estos, el cotejo, o la interconexión, así como su bloqueo, supresión o destrucción, intercambio o digitalización de datos personales, entre otros.

Sin embargo, no consta descrito el derecho a no soportar valoraciones de procesos automatizados.

f. Derecho de consulta al registro general de protección de datos personales

De acuerdo con el artículo 44 del reglamento, Decreto Ejecutivo 37554, las personas físicas o jurídicas propietarias de bases de datos personales, deberán inscribirlas mediante un registro ante la Agencia, suministrando la siguiente información: solicitud del propietario físico o jurídico, debidamente autenticado notarialmente o confrontada la firma. En el caso de persona jurídica, deberá presentarse personería jurídica vigente con máximo un mes de haber sido expedida; designación del responsable de la base de datos personales ante la Agencia y ante terceros, con indicación del medio y lugar de contacto, así como carta de aceptación del cargo; también identificación de los encargados, incluyendo sus datos de contacto, así como carta de aceptación del cargo, este último reformado por el artículo 9° del decreto ejecutivo en el 2016; además nombres de las bases de datos y su ubicación física; especificación de las finalidades y los usos previstos, este último reformado por el artículo 9° de decreto ejecutivo en el 2016; tipos de datos personales sometidos a tratamiento en dichas bases de datos; procedimientos de obtención de los datos personales, este último reformado por el artículo 9° de decreto ejecutivo en el 2016; descripción técnica de las medidas de seguridad que se utilizan en el tratamiento de los datos personales; los destinatarios de transferencias de los datos personales; copia de los protocolos mínimos de actuación, este último reformado por el artículo 9° de decreto ejecutivo en el 2016, listado de los contratos globales y ventas de ficheros vigentes, así como indicación de la estimación pecuniaria de cada uno de esos contratos; señalamiento de fax o correo electrónico para recibir notificaciones de la Agencia. Asimismo, el responsable deberá mantener el registro de la base de datos, en todo momento, actualizados ante la Agencia. Sin embargo, no serán sujetas de inscripción ante la Agencia, las bases de datos personales, internas o domésticas. Este último adicionado por el artículo 9° de decreto ejecutivo en el 2016.

Por otra parte, el artículo 46 declara que la Agencia puede realizar inspecciones administrativas o de oficio, con el fin de verificar posibles infracciones; si este es el caso el responsable deberá levantar un acta. En similar sentido, la Agencia podrá acceder a las bases sin restricción alguna cuando exista una denuncia o se habilite evidencia que presente un mal manejo de las mismas; para esto, la Agencia debe establecer lineamientos que regulen el secreto profesional y para todo proceso llevar una bitácora que contenga mínimamente el motivo, los accesos y consultas realizadas y el funcionario asignado.

Por su lado, el artículo 48 regula el procedimiento de inscripción determinando que inicia con la solicitud ante la Agencia y su posterior plazo de veinte días hábiles para verificar los requisitos de forma y fondo presentados. Si estos no son los correctos, el artículo 49 establece que la Agencia requerirá al solicitante que en el plazo de 10 días hábiles subsane la omisión; sin embargo, si los requisitos han sido cumplidos según el artículo 50 conferirá al solicitante el mismo plazo para que cancele el canon anual, si lo uno o lo otro no sucede en el plazo establecido se archivará, sin perjuicio a la opción de presentarse una nueva solicitud.

Conforme al artículo 51, si el pago se ha efectuado el Director de la Agencia dictará dentro del plazo de diez días hábiles la resolución de inscripción del registro de la base de datos ante la Agencia, lo cual no exime al responsable del cumplimiento y seguimiento del resto de obligaciones previstas en la ley. La resolución aquí expresada, con base en el artículo 52, deberá contener: el código asignado por la Agencia a la base de datos; el nombre de la base de datos inscrita y la ubicación de los datos; la identificación del responsable de la base de datos personales y su medio de contacto; la identificación del encargado y su medio de contacto; la categoría de los datos personales que contiene; los procedimientos de obtención de los datos y la finalidad de su tratamiento.

De acuerdo con lo dispuesto en el artículo 53, dentro de veinte días hábiles a partir de la presentación de la solicitud, el Director de la agencia puede dictar resolución denegándola cuando en el análisis de los requisitos se determine la improcedencia de la misma.

Por otra parte, conforme al artículo 54, la información inscrita en el registro de la base de datos deberá mantenerse actualizada. De ese modo, cualquier información que afecte a su contenido deberá ser comunicada por el responsable a la Agencia dentro del plazo de cinco días hábiles.

Asimismo, si el propietario o el responsable de la base de datos decide cancelarla del registro, según el artículo 55, deberá presentarse una solicitud a la Agencia que determine las previsiones para la eliminación, supresión o destrucción de los datos personales. Paso seguido, la Agencia tendrá un mes para proceder con la cancelación.

g. Derecho a indemnización por daños causados

No consta con la denominación de derecho a indemnización por daños causados ni en la ley ni en el reglamento.

h. Derecho a la confidencialidad

Se define al deber de confidencialidad en el artículo 3 de la Ley 8968, como la obligación de los responsables de bases de datos, personal a su cargo y personal de la Prodhab, de guardar la confidencialidad principalmente ante el acceso de información de datos personales y sensibles, aun después de terminada su relación con la base de datos. Encausado en este criterio, el artículo 11 advierte lo mismo bajo el nombre de secreto profesional o funcional, y declara que se podrá exceptuar de esto solo bajo decisión judicial en lo estrictamente necesario.

Sobre el reglamento, Decreto Ejecutivo 37554, el artículo 2 define garantía de confidencialidad en el mismo criterio que lo hace la ley, aunque aquella lo llame deber, y esta última se aclare específicamente que debe ser cumplido por los responsables de los ficheros, estos son persona física o jurídica, pública o privada.

i. Derecho al olvido digital

Según conviene el artículo 11 del reglamento, Decreto Ejecutivo 37554, reformado por el artículo 5 del decreto ejecutivo de 2016, bajo la rúbrica derecho al olvido consta que no se puede exceder a diez años la conservación de datos personales que puedan afectar a su titular, a partir del fin del tratamiento de los mismos, salvo disposición normativa, que por el acuerdo de partes se haya establecido otro plazo, que exista relación continuada entre las partes o que medie interés público para conservar el dato.

j. Spam

No consta con la denominación de spam ni en la ley ni en el reglamento. Sin embargo, aparece como delito en el Código Penal con el texto siguiente:

> Artículo 232.- Instalación o propagación de programas informáticos maliciosos.- Será sancionado con prisión de uno a seis años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos. La misma pena se impondrá en los siguientes casos: [...] **e)** A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.[1487]

k. Divulgación

Concorde con lo establecido en el artículo 22 de la Ley 8968, la Prodhab elaborará una estrategia de comunicación que permita que los administrados conozcan los derechos y mecanismos de defensa que tienen derivados del manejo de sus datos personales, mediante actividades de divulgación. Además, promoverá la protección de dicha información entre las personas o empresas que la recolecten.

[1487] Asamblea Legislativa de la República de Costa Rica, "Ley: 9048 del 10/07/2012. Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal", *Sistema Costarricense de Información Jurídica*, accedido 17 de noviembre de 2017, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=101586&param2=2&strTipM=TC&lResultado=13&strSim=simp.

l. Derecho a la revocación

Según lo establece el artículo 7 del reglamento, Decreto Ejecutivo 37554, el titular puede revocar el consentimiento para el tratamiento de sus datos personales, en cualquier momento mediante mecanismos ofrecidos por el responsable. Cuando este haya recibido la solicitud de revocación contará con cinco días hábiles para proceder conforme a esta, y deberá informales de dicho proceso a todas aquellas personas físicas o jurídicas a quienes se les haya transferido los datos, para que ejecuten de igual manera la revocación del consentimiento durante cinco días hábiles, según el artículo 8, que también afirma que la revocación no tendrá efecto retroactivo.

Por otra parte, a partir de la presentación de dicha solicitud, el responsable deberá responder de forma gratuita en el plazo de tres días hábiles conforme lo propuesto en el artículo 9. Y en el mismo sentido, según el artículo 10, en caso de negativa por parte del responsable, el titular podrá presentar ante la Agencia la denuncia correspondiente.

g) Procedimientos

Conforme señala el artículo 13 de la Ley 8968, toda persona interesada tiene derecho a un procedimiento administrativo sencillo y rápido ante la Prodhab, con el fin de ser protegido contra actos que violen sus derechos fundamentales reconocidos por esta ley; dicho procedimiento se manifiesta en los varios procesos administrativos que se analizan a continuación.

a. *Sujeto activo:* Según al artículo 15 del reglamento, Decreto Ejecutivo 37554, los derechos de acceso, rectificación, modificación, revocación o eliminación, se ejercerán por el titular o su representante, con acreditación previa de esos títulos.

b. *Sujeto pasivo:* El responsable, conforme el artículo 16 del Decreto Ejecutivo 37554, deberá poner a disposición del titular, los medios de comunicación que considere acertados, motivo por el cual el titular debe en la solicitud de acceso, rectificación, modificación, revocación o eliminación, indicar el medio para recibir notificaciones según lo decreta el artículo 17, y detalla que en caso de no cumplir con este requisito, opera la notificación automática señalada en la Ley de Notificaciones Judiciales.

   El artículo 18 del Decreto Ejecutivo 37554 establece que el responsable deberá atender y tramitar toda solicitud para el ejercicio de los derechos personales del titular en un plazo de cinco días hábiles, a partir del día siguiente en que haya sido recibida, en cuyo caso el responsable anotará la correspondiente fecha de recepción en el acuse de recibo que entregue al titular. Y añade que solo se verá interrumpido el plazo en caso de que el responsable requiera información adicional al titular, tal como lo desarrolla el artículo 19, en donde acopia que solo se podrá requerir por una vez y dentro de los cinco días hábiles siguientes a la recepción de la solicitud; por su parte, el titular tiene el mismo plazo para atender el requerimiento y, después de hacerlo, el responsable contará con cinco días hábiles para dar respuesta a la solicitud; sin embargo, si el titular no da respuesta a los

requerimientos en dicho plazo, se tendrá por no presentada la solicitud correspondiente.

De conformidad con lo desarrollado el artículo 20, se establece que en todos los casos el responsable deberá dar respuesta a las solicitudes que reciba del titular, con independencia de que figuren o no datos personales de este en sus bases de datos, de conformidad con el plazo determinado y refiriéndose sobre la totalidad del registro perteneciente al mismo; además, deberá presentarse en un formato legible, comprensible y de fácil acceso. Se concluye que este informe en ningún caso podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el titular solicitante.

c. *Procedimiento para consultas*: Para estos efectos el artículo 21 del reglamento, Decreto Ejecutivo 37554, dispone que se podrá realizar las consultas de información con un intervalo mínimo de seis meses, salvo que de manera fundamentada el titular exprese al responsable los motivos por los cuales considera que se ha violentado sus derechos. En caso de que el responsable considere que los motivos no son de recibo y existiera la posibilidad de un uso abusivo sobre ese derecho, la solicitud se elevará ante la Prodhab en los siguientes cinco días hábiles, la cual tendrá diez días hábiles para resolverlo. Y el artículo 22 del mismo apartado sustenta la negativa del responsable advirtiendo que deberá ser presentada por escrito y debidamente justificada; en esta situación el titular puede también acudir a la Agencia.

d. *Procedimiento contra la inscripción final de base de datos*: Según el artículo 56, se procede contra la resolución final dentro del tercer día hábil a partir de la respectiva notificación del acto final, la interposición ante la Agencia de los Recursos ordinarios de Reconsideración y Apelación; siendo potestativo usar ambos recursos o uno solo de ellos, pero será inadmisible el que se interponga pasado dicho plazo.

e. *Procedimiento del recurso de reconsideración*: Para concluir con este apartado, según el artículo 57 del Decreto Ejecutivo 37554, el recurso de reconsideración será resuelto por la Agencia dentro de los ocho días hábiles posteriores a su presentación; y el recurso de apelación deberá remitir el mismo y el respectivo expediente al Ministro de Justicia y Paz dentro de los siguientes tres días hábiles, a partir de la notificación de la resolución del recurso de reconsideración. El Ministro de Justicia y Paz deberá resolver el recurso de apelación dentro del plazo de ocho días hábiles posteriores al recibo del expediente.

f. *Procedimiento de protección de derechos*: Cualquier persona que ostente un derecho subjetivo o un interés legítimo puede denunciar, ante la Prodhab, que una base de datos pública o privada actúa en contravención de las reglas o los principios básicos para la protección de los datos y la autodeterminación informativa establecidas en esta ley conforme el texto del artículo 24 de la Ley 8968. Asimismo, el artículo 25 señala el trámite pertinente para estas denuncias, otorgándole al responsable de la base de datos un plazo de tres días hábiles para que se pronuncie acerca de la

veracidad de tales cargos. La persona denunciada deberá remitir los medios de prueba que respalden sus afirmaciones junto con un informe, que se considerará dado bajo juramento. Se añade que la omisión de rendir el informe en el plazo estipulado hará que se tengan por ciertos los hechos acusados. De igual manera, la Prodhab podrá efectuar inspecciones *in situ* en sus bases de datos. Para amparar los derechos de la persona interesada, puede decretar medidas cautelares que cercioren el efectivo resultado del procedimiento. Se dictará el acto final a más tardar después de un mes de la presentación de la denuncia; cabrá el recurso de reconsideración dentro del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido.

Por su parte, el reglamento del Decreto Ejecutivo 37554, en el artículo 58, determina texto idéntico al del artículo 24 de la ley, pero además señala que la Agencia podrá iniciar un procedimiento que verifique si una base de datos está siendo utilizada dentro de estos términos, aplicando los principios establecidos en el Libro Segundo de la Ley General de la Administración Pública.

Dentro de este margen el artículo 59, señala que el procedimiento de protección de derechos procederá cuando: se recolecten datos personales para su uso sin que se le conceda amplia información a la persona interesada; se recolecten, almacenen y transmitan datos personales por medio de herramientas que no garanticen la seguridad e inalterabilidad de los mismos, sin el consentimiento informado y expreso de su titular o sin ley o norma especial que lo autorice, y si tiene una finalidad distinta a la autorizada por él; se transfieran datos personales a otras personas o empresas en contravención de las reglas; se niegue injustificadamente a dar acceso a un titular sobre los datos que consten en archivos y bases de datos, a fin de verificar su calidad, recolección, almacenamiento y uso; se niegue injustificadamente a eliminar o rectificar los datos de una persona que así lo haya solicitado por medio claro e inequívoco; se obtengan de los titulares o terceros, datos personales por medio de engaño, violencia, dolo, mala fe o amenaza; se revele información registrada en una base de datos personales cuyo secreto esté obligado a guardar; se proporcione a un tercero, información falsa o distinta contenida en un archivo de datos; se realice tratamiento de datos personales sin encontrarse debidamente inscrito ante la Agencia; se transfieran, a las bases de datos de terceros países, información de carácter personal de los costarricenses o de los extranjeros radicados en el país, sin el consentimiento de sus titulares y por otras causas que a juicio de la Agencia afecten los derechos del titular conforme a la ley y al presente reglamento.

Así también, el artículo 62 declara que la Agencia podrá prevenir al titular para que en diez días hábiles aclare y precise la información o documentación presentada, bajo la pena de inadmisibilidad de la denuncia y su consecuente archivo.

Según el artículo 63, la Agencia deberá resolver sobre la admisibilidad de la solicitud de protección del derecho del titular, en un plazo de cinco días

hábiles a partir de la recepción o subsanación de la denuncia. Contra esta procede, dentro del tercer día hábil a partir de la respectiva notificación, la interposición ante la Agencia de los Recursos ordinarios de Reconsideración y Apelación, siendo potestativo usar ambos o solo uno de ellos, pero será inadmisible el que se interponga pasado dicho plazo. De modo que los recursos interpuestos deberán ser resueltos, el de reconsideración por la Agencia dentro de los ocho días hábiles posteriores a su presentación, y en caso de haberse interpuesto el recurso de apelación deberá remitir el mismo y el respectivo expediente al Ministro (a) de Justicia y Paz dentro de los siguientes tres días hábiles, a partir de la notificación de la resolución del recurso de reconsideración. El Ministro de Justicia y Paz deberá resolver el recurso de apelación dentro del plazo de ocho días hábiles posteriores al recibo del expediente.

Por su parte el artículo 64 advierte que en casos especiales y en cualquier momento la Agencia podrá disponer las medidas cautelares que estime necesarias para el cumplimiento de la protección de los derechos personales de un titular, respecto del tratamiento de sus datos, basada en el principio de proporcionalidad, los caracteres de instrumentalidad y provisionalidad, así como ponderar los eventuales daños y perjuicios que se provoquen con la medida a las partes. Para el desarrollo de tales efectos, la Agencia dará audiencia por veinticuatro horas al responsable de la base de datos. Transcurrido dicho plazo, la Agencia deberá resolver sobre la medida en un plazo máximo de tres días hábiles.

En esa consideración, el artículo 65 afirma que contra la resolución que resuelve la medida cautelar cabrá únicamente el recurso de reconsideración ante la Agencia, que deberá interponerse dentro del plazo de veinticuatro horas a partir de la notificación. La Agencia resolverá el recurso dentro del plazo de tres días hábiles a partir de la interposición del recurso. Se añade en el artículo 66 que sobre la aplicación de las respectivas medidas cautelares, la Agencia ponderará los intereses en juego y deberá constatar que se esté en presencia de los siguientes presupuestos: apariencia de buen derecho, daño inminente de difícil reparación, la no afectación al interés público.

Posteriormente, según reza el artículo 67, admitida la denuncia la Agencia hará el traslado de cargos a quien corresponda, para que dentro del plazo de tres días hábiles informe sobre la veracidad de los cargos y aporte la prueba que estime pertinente. Las manifestaciones realizadas se considerarán dadas bajo fe de juramento. Además, la omisión de rendir informe en el plazo estipulado hará que se tengan por ciertos los hechos acusados.

g. *Efectos de la resolución estimatoria*: Dentro del mismo margen, con base en el artículo 26 del Decreto Ejecutivo 37554, se establece que la información del interesado es falsa, incompleta, inexacta, o bien que esta fue indebidamente recolectada, almacenada o difundida; deberá decretarse su inmediata supresión, rectificación, adición o aclaración, o bien impedimento respecto de su transferencia o difusión. De la misma manera, si la persona denunciada no cumple íntegramente lo dispuesto, estará sujeta a las sanciones previstas.

h) Recurso de amparo

Conforme señala el artículo 13 de la Ley 8968, se determina que pese a la vía administrativa, existen garantías jurisdiccionales generales o específicas que han sido establecidas en salvaguarda del derecho a la protección de datos personales; entre ellas la acción de amparo que fue utilizada y que permitió el desarrollo jurisprudencial hasta la promulgación de la Ley 8968.

En tal sentido, la Ley 7135, 11/10/1989, Ley de la Jurisdicción Constitucional, Asamblea Legislativa, con la reforma realizada al 31/10/2011, concibe una acción de carácter constitucional que puede ser utilizada en la acción de amparo.

a. Sujeto activo

El artículo 33 de la Ley 7135 determina que cualquier persona podrá interponer el recurso de amparo.

b. Sujetos pasivos u obligados

Por su parte, el artículo 34 de la Ley 7135 señala que el recurso de amparo podrá dirigirse contra el servidor o el titular del órgano que aparezca como presunto autor del agravio. Si uno u otro hubiesen actuado en cumplimiento de órdenes o instrucciones impartidas por un superior, o con su autorización o aprobación, se tendrá por establecido el amparo contra ambos, sin perjuicio de lo que se decida en sentencia. De ignorarse la identidad del servidor, el recurso se tendrá por establecido contra el jerarca.

c. Derechos tutelados por el recurso de amparo

El artículo 29 de la Ley 7135 determina que el recurso de amparo garantiza los derechos y libertades fundamentales a que se refiere esta ley, salvo los protegidos por el de *habeas corpus*. Es decir, aquellos constantes en la Constitución de la República de Costa Rica, el Derecho Internacional o Comunitario vigente. Se aclara que la Sala Constitucional reconoce el derecho a la protección de datos personales mediante las resoluciones que por acción de amparo constantes en las sentencias 4154-97, 7175-97, 4347-99 y 5802-99, analizadas previamente.

d. Procedencia del recurso de amparo

El artículo 29 de la Ley 7135 determina que el recurso de amparo procede contra toda disposición, acuerdo o resolución y, en general, contra toda acción, omisión o simple actuación material no fundada en un acto administrativo eficaz, de los servidores y órganos públicos, que haya violado, viole o amenace violar cualquiera de aquellos derechos.

e. Procedimiento del recurso de amparo

Conforme el artículo 39, la tramitación del recurso estará a cargo del Presidente de la Sala o del magistrado a quien este designe, y se sustanciará en forma privilegiada, para

lo cual se pospondrá cualquier asunto de naturaleza diferente, salvo el de *habeas corpus*. Los plazos son perentorios e improrrogables, sin perjuicio de lo dispuesto en el artículo 47.

i) Institucionalidad de protección

La Agencia de protección de Datos de los Habitantes[1488] es un ente adscrito al Ministerio de Justicia y Paz, que entró en funcionamiento el 5 de marzo del 2013 a partir de la vigencia del Reglamento a la Ley 8968.

De conformidad con lo señalado en el artículo 15, se crea el la Agencia de Protección de Datos de los habitantes (Prodhab). Este órgano es de carácter desconcentrado máximo adscrito al Ministerio de Justicia y Paz que tiene personalidad jurídica instrumental propia en el desempeño de las funciones que le asigna esta ley, además de la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones. La Agencia goza de independencia de criterio.

Las atribuciones se encuentran establecidas en el artículo 16 entre las que destacan, el velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos, llevar un registro de las bases de datos reguladas por esta ley; requerir, a quienes administren bases de datos, las informaciones necesarias para el ejercicio de su cargo, entre ellas, los protocolos utilizados, resolver sobre los reclamos por infracción a las normas sobre protección de los datos personales, esto es la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en los archivos y las bases de datos, cuando estas contravengan las normas sobre protección de los datos personales; imponer sanciones; dictar directrices necesarias, entre otras.

j) Régimen sancionador

La descripción de las sanciones se encuentra en el artículo 28 de la Ley 8968, que las clasifica en faltas leves, graves y gravísimas. Las primeras, faltas leves, atinentes a la recolección, almacenaje, y transmisión de datos personales para su uso en base de datos sin que se le otorgue suficiente y amplia información a la persona interesada o no se garanticen la seguridad e inalterabilidad de los datos.

En cambio, las faltas graves se refieren a la recolección, almacenaje, transmisión o tratamiento, cesión sin el consentimiento informado y expreso del titular de los datos, con arreglo a las disposiciones de esta ley.

Finalmente, por faltas gravísimas constan aquellas por las cuales se sanciona a quien recolecta, almacena, transmite o de cualquier otra forma emplea, por parte de personas físicas o jurídicas privadas, datos sensibles.

La Ley 8968 determina como régimen sancionatorio para bases de datos públicas, el cual se activa cuando la persona responsable de una base de datos pública comete

[1488] Agencia de Protección de Datos de los Habitantes Prodhab, Sitio web institucional de la Agencia de Protección de Datos de los Habitantes Prodhab, accedido 1 de octubre de 2017, http://www.prodhab.go.cr/.

alguna de las faltas anteriores. Por eso, la Prodhab dictará una resolución estableciendo las medidas que proceda adoptar para que cesen o se corrijan los efectos de la falta. Lo anterior sin perjuicio de la responsabilidad penal en que haya incurrido.

Conforme a lo estipulado en el artículo 27 de la Ley 8968, la Prodhab podrá iniciar un procedimiento para determinar si una base de datos está siendo empleada de conformidad con sus principios; para lo cual seguirá el procedimiento ordinario previsto en la Ley General de la Administración Pública. Contra el acto final cabrá recurso de reconsideración dentro del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido.

k) Transferencia internacional de datos

Consta en el artículo 14 la norma expresa que regula la transferencia de datos personales, públicas o privadas, que solo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado, expresa y válidamente, tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley.

l) Protocolos de actuación

Característica propia de la normativa costarricense es el artículo 12 que establece la posibilidad de que se incorporen Protocolos de actuación, en el cual se describan los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales. Añadiéndose que para que sean válidos los protocolos de actuación deberán ser inscritos, así como sus posteriores modificaciones, ante la Prodhab. La Prodhab podrá verificar, en cualquier momento, que la base de datos cumpla cabalmente con los términos de su protocolo.

m) Características y prohibiciones del personal de la Agencia

Otra de las características peculiares de la normativa costarricense es el constante en el artículo 18 que señala que el personal técnico y administrativo de la Prodhab está obligado a guardar secreto profesional y deber de confidencialidad de los datos de carácter personal que conozca en el ejercicio de sus funciones. Que no podrán prestar servicios a las personas o empresas que se dediquen al acopio, el almacenamiento o el manejo de datos personales. Dicha prohibición persistirá hasta dos años después de haber cesado sus funciones. Asimismo, no podrán revelar o de cualquier forma propalar los datos personales a que ha tenido acceso con ocasión de su cargo. Esta prohibición persistirá indefinidamente aun después de haber cesado en su cargo.

2.17 El Salvador

La Constitución de la República de El Salvador de 1983, con reformas hasta 2009,[1489] únicamente reconoce el derecho a la intimidad personal y familiar de conformidad con lo constante en el texto siguiente:

[1489] Asamblea Legislativa de la República de El Salvador, "Constitución de la República de El Salvador de 1983 con reformas hasta 2009", *Political Database of the Americas*, accedido 28 de enero de 2018, http://pdba.georgetown.edu/Constitutions/ElSal/elsalvador.html.

> Artículo 2.- *Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa de los mismos. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*[1490]

Ahora bien, la Corte Suprema de Justicia del Salvador reconoce por primera vez a la protección de datos personales, autodeterminación informativa o intimidad informática como derecho fundamental, así como su contenido, en la sentencia de amparo constitucional 118-2002 (ítem: 33366), interpuesto en contra de una empresa dedicada a la recopilación y comercialización de información crediticia, como se transcribe a continuación:

> Frente al peligro anteriormente advertido existe una manifestación del derecho a la intimidad, que es precisamente el derecho a la protección de los datos y consiste en que el individuo pueda controlar el uso o tratamiento de los mismos, a fin de impedir una lesión a su esfera jurídica. Tal derecho ha sido denominado de diversas formas, según el autor que lo formule; y así, se le conoce como derecho a la autodeterminación informativa o derecho a la intimidad informática; pero, indistintamente de su formulación, éste debe ser entendido como aquel que tiene por objeto preservar la información individual que se encuentra contenida en registros públicos o privados, especialmente la almacenada a través de los medios informáticos, frente a su utilización arbitraria. De modo que a partir del acceso a la información, exista la posibilidad de solicitar la corrección, actualización, modificación y eliminación de los mismos. Se puede afirmar entonces que el derecho a la intimidad en el ámbito informático implica lo siguiente: (a) que todo individuo tiene derecho de acceder a la información personal y especialmente a aquella que se encuentre contenida en bancos de datos informatizados; (b) que todo individuo ha de tener la posibilidad y el derecho a controlar, de forma razonable, la transmisión o distribución de la información personal que le afecte, (c) que debe existir, en el ordenamiento jurídico, un proceso o recurso que permita hacer efectivos los puntos señalados. Todo ello con la finalidad de establecer la estructura mínima que permita el manejo fiable de los datos personales de los individuos que se encuentren en banco de datos mecánicos o informáticos para conservar la veracidad, integridad y actualidad de los mismos; así como la regulación sobre la inaccesibilidad de otras instancias que no comprueben la existencia de una finalidad que justifique suficientemente la pretensión de conocerlos.[1491]

Posteriormente, se intentó que mediante el pronunciamiento 36-2004 de la Corte Suprema de Justicia se declare la inconstitucionalidad por omisión en que incurre el órgano legislativo, en tanto que no ha desarrollado legalmente los mecanismos idóneos de protección del derecho a la autodeterminación informativa. Sin embargo, el tribunal señaló que:

> [...] no existe la inconstitucionalidad por omisión, al no desarrollar legalmente los mecanismos idóneos de protección del derecho a la autodeterminación informativa –entendidos éstos como el habeas data como proceso especializado y la emisión de un cuerpo normativo que sistematice las regulaciones relativas al mencionado derecho constitucional, incluyendo la creación de un ente administrativo encargado de dicha

[1490] Ibíd.

[1491] Corte Suprema de Justicia de República de El Salvador, "Amparo 118-2002", *Centro de Documentación Judicial 2016*, accedido 4 de febrero de 2018, https://bit.ly/2CwIRdX.

> competencia–, por tratarse de aspectos que pertenecen al ámbito de libertad de configuración del legislador.[1492]

Finamente, en sentencia de amparo 934-2007 se acciona por supuestas acciones lesivas al derecho constitucional a la autodeterminación informativa contra actuaciones y omisiones de Infornet, S.A. de C.V., la cual, según la parte demandante, se dedica a la "recopilación y comercialización ilegítima, inconstitucional e indiscriminada de la información personal, crediticia, judicial, mercantil y de prensa, de aproximadamente cuatro millones de salvadoreños. Lo que permite, además, la creación de perfiles por medio de los bancos de datos informáticos de fácil acceso, manejo y transferencia, con el objeto de venderlos al mejor postor y lo anterior, sin el consentimiento expreso de los titulares de dichos datos".

La Corte Suprema de Justicia de la República del Salvador declaró procedente el amparo y condena por violación al derecho a la autodeterminación informativa a Infornet, S.A. de C.V. Le ordenó que, de forma gratuita, permita a los particulares interesados el acceso a la base de datos que tiene en su poder, con el objeto de que puedan actualizar, rectificar o anular aquellos datos estrictamente personales que no constan en registros públicos –y de los que por ley tengan el carácter de reservados–; o que, constando en dichos registros, no estén actualizados. Además, señaló que debe abstenerse de utilizar y transferir a cualquier título y destino la información que consta en su base, referida a los datos estrictamente personales, a menos que en cada caso, tenga la autorización o el consentimiento expreso de su titular, so pena de incurrir en la responsabilidad legal correspondiente.[1493]

La ley en la que se menciona aspectos que desarrollan el derecho a la protección de datos personales, pero únicamente en el ámbito de lo público, es el Decreto 534, 8 de abril de 2011, Ley de Acceso a la Información pública de El Salvador.[1494] Y el Decreto 136-2011, reglamento a la Ley de Acceso a la Información Pública de El Salvador .[1495]

Asimismo, el Manual Operativo de Protección de Datos en el Salvador de 2015 establece guías, directrices e insumos para operativizar la protección de datos en El Salvador, ante la ausencia de una normativa específica.[1496]

A continuación se analizará sobre el contenido esencial, aclarando que por cuanto la normativa existente solo cobija ficheros públicos, es un análisis sesgado al ámbito público exclusivamente.

[1492] Corte Suprema de Justicia de República de El Salvador, "Amparo 36-2004", *Centro de Documentación Judicial 2016*, accedido 4 de febrero de 2018, https://bit.ly/2CwIRdX.

[1493] Corte Suprema de Justicia de República de El Salvador, "Amparo 934-2007", *Centro de Documentación Judicial 2016*, accedido 4 de febrero de 2018, https://bit.ly/2CwIRdX.

[1494] Asamblea Legislativa de la República de El Salvador, "Ley de Acceso a la Información Pública, Decreto 534 de 8 de abril de 2011", *Gobierno Abierto de El Salvador*, 2011, accedido 28 de enero de 2018, https://www.gobiernoabierto.gob.sv/pages/ley-de-acceso-a-la-informacion-publica.

[1495] Presidencia de la República de El Salvador, "Decreto 136-2011, reglamento a la Ley de Acceso a Información Pública de El Salvador", accedido 28 de enero de 2018, http://www.oas.org/juridico/PDFs/mesicic4_slv_regla.pdf.

[1496] A. CHIRINO SÁNCHEZ, *Manual Operativo de Protección de Datos en el Salvador* (Madrid, 2015), accedido 28 de enero de 2018, http://sia.eurosocial-ii.eu/files/docs/1432887451-DT_26_Chirino.pdf.

b) Ámbito: Registros o ficheros públicos y privados

La Ley 534-2011, Ley de Acceso a la Información Pública de El Salvador, según el artículo 3, literal h), referido a las finalidades de la ley señala, entre ellas, la de proteger los datos personales en posesión de los entes obligados y garantizar su exactitud.

c) Naturaleza del dato

Conforme la citada Ley 534-2011, se considera dato personal aquel que se refiere a información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra análoga, de conformidad con el artículo 6.

Además, se considera dentro de las clasificaciones de datos aplicables la de datos personales sensibles, que son aquellos que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral y familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, a la intimidad personal y familiar y a la propia imagen, al tenor del artículo 6 antes citado.

d) Sujeto activo

El artículo 31 de la Ley 534-2011, referido al conocimiento sobre la finalidad de los usos de los datos personales, menciona la frase "toda persona", por lo que pudiera entenderse como titulares de estos derechos, tanto a personas naturales como jurídicas. Además, en su parte final determina que el acceso a los datos personales es exclusivo de su titular o su representante. De esta forma, se establece la titularidad de los datos personales como elemento sustancial para solicitar el ejercicio de este derecho.

La aclaración antes citada permite concluir que para el caso de datos personales no se aplica el artículo 9 de la ley citada, la cual menciona expresamente que el ejercicio de los derechos establecidos en esta ley corresponde a toda persona, por sí o por medio de su representante, sin necesidad de acreditar interés legítimo o derecho precedente.

e) Sujeto pasivo

Por el ámbito limitado de esta ley, se entiende que los sujetos pasivos serán únicamente las entidades públicas como entes obligados para garantizar la exactitud de los datos personales (art. 3, literal h), Ley 534-2011.

En el artículo 7 de la Ley 534-2011, en el apartado "Entes obligados" señala que:

> Están obligados al cumplimiento de esta ley los órganos del Estado, sus dependencias, las instituciones autónomas, las municipalidades o cualquier otra entidad u organismo que administre recursos públicos, bienes del Estado o ejecute actos de la administración pública en general. Se incluye dentro de los recursos públicos aquellos fondos provenientes de Convenios o Tratados que celebre el Estado con otros Estados o con

Organismos Internacionales, a menos que el Convenio o Tratado determine otro régimen de acceso a la información.

También están obligadas por esta ley las sociedades de economía mixta y las personas naturales o jurídicas que manejen recursos o información pública o ejecuten actos de la función estatal, nacional o local tales como las contrataciones públicas, concesiones de obras o servicios públicos. El ámbito de la obligación de estos entes se limita a permitir el acceso a la información concerniente a la administración de los fondos o información pública otorgada y a la función pública conferida, en su caso.

En consecuencia, todos los servidores públicos, dentro o fuera del territorio de la República, y las personas que laboren en las entidades mencionadas en este artículo, están obligados al cumplimiento de la presente ley.

f) Objeto o bien jurídico

a. Derecho de información

En la descripción del contenido del derecho a la protección de datos personales, el artículo 31 de la Ley 534-2011 señala que: "Toda persona, directamente o a través de su representante, tendrá derecho a saber si se están procesando sus datos personales; [...] a conocer los destinatarios cuando esta información sea transmitida, permitiéndole conocer las razones que motivaron su petición, en los términos de esta ley". De modo que se establece el derecho de las personas a ser informadas respecto de si se están procesando datos personales de los cuales es titular y por qué y a quién fueron estos transmitidos.

b. Autodeterminación informativa

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho. Su reconocimiento, como vio en líneas anteriores, se realiza mediante precedentes jurisprudenciales dictados por la Corte Suprema de Justicia del El Salvador según resoluciones de Amparo 118-2002,[1497] Acción de inconstitucionalidad 36-2004[1498] y de Amparo 934-2007.[1499]

c. Necesidad de mandato legal para tratamiento sin autorización del titular

El artículo 34 de la Ley 534-2011 determina que los entes obligados deberán proporcionar o divulgar datos personales, aun sin el consentimiento del titular; es decir, amparados en la disposición legal señalada, en los casos siguientes: a. Cuando fuere necesario por razones estadísticas, científicas o de interés general, siempre que no se identifique a la persona a quien se refieran. b. Cuando se transmitan entre entes obligados, siempre y cuando los datos se destinen al ejercicio de sus facultades. c. Cuando se trate de la investigación de delitos e infracciones administrativas, en cuyo caso se seguirán los procedimientos previstos en las leyes pertinentes. d. Cuando exista orden judicial. e. Cuando contraten o recurran a terceros para la prestación de un servicio que demande el tratamiento de datos personales. Los terceros no podrán utilizar

[1497] Corte Suprema de Justicia de República de El Salvador, "Amparo 118-2002".
[1498] Corte Suprema de Justicia de República de El Salvador, "Amparo 36-2004".
[1499] Corte Suprema de Justicia de República de El Salvador, "Amparo 934-2007".

los datos personales con propósitos distintos a aquellos para los cuales se les hubieren proporcionado y tendrán las responsabilidades legales que genere su actuación.

d. Principios

i. Deber de información

En líneas anteriores hicimos referencia al derecho de información; pero respecto al deber de información, no consta en la normativa constitucional ni legal salvadoreña.

ii. Pertinencia

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho.

iii. Calidad

El artículo 32 de la Ley 534-2011 determina que los entes obligados públicos serán responsables de proteger los datos personales y, en relación con estos, procurarán que los datos personales sean exactos y actualizados.

Los criterios de actualidad y precisión son aquellos que determinan que los datos personales cumplan con el principio de calidad.

iv. Finalidad

El artículo 32 de la Ley 534-2011 determina que los entes obligados públicos serán responsables de proteger los datos personales y, en relación con estos, deberán usar los datos exclusivamente en el cumplimiento de los fines institucionales para los que fueron solicitados u obtenidos. Es decir, se cumple con esta disposición, aunque de manera general y aplicable al ámbito público, exclusivamente el principio de finalidad.

v. Seguridad

El artículo 32 de la Ley 534-2011 determina que los entes obligados públicos serán responsables de proteger los datos personales y, en relación con estos, deberán adoptar medidas que protejan la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

Aunque no se mencionan los niveles de seguridad, ni los mecanismos aplicables, la normativa describe las posibles transgresiones que desde la seguridad de los datos personales deben ser salvaguardas.

vi. Consentimiento

El artículo 33 de la Ley 534-2011 señala que los entes obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información administrados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso y libre, por escrito o por un medio equivalente, de los individuos a que haga referencia la información.

No se hace mención ni a la condición de previo ni de informado de este consentimiento para su validez.

g) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

a. Derecho de acceso

En la descripción del contenido del derecho a la protección de datos personales, el artículo 31 de la Ley 534-2011 señala que Toda persona, directamente o por intermedio de su representante, tendrá derecho a conseguir una reproducción inteligible de ella sin demora; anotándose que el acceso a los datos personales es exclusivo de su titular o su representante.

Asimismo, el artículo 32 determina que los entes obligados serán responsables de proteger los datos personales y, en relación con estos, deberán adoptar procedimientos adecuados para recibir y responder las solicitudes de indagatoria, actualización, modificación y supresión de datos personales.

En otras palabras, mediante los artículos 31 y 32 se determina condiciones para el ejercicio de una versión limitada de derecho de acceso al mencionar la obligación de las entidades de establecer procedimientos adecuados para solicitar y para entregar información por medio de reproducciones inteligibles y sin demora.

b. Derecho de rectificación

Asimismo, el artículo 32 determina que los entes obligados serán responsables de proteger los datos personales y, en relación con estos, deberán adoptar procedimientos adecuados para recibir y responder las solicitudes de indagatoria, actualización, modificación y supresión de datos personales; además de rectificar o completar los datos personales que fueren inexactos o incompletos.

Es decir, los entes obligados deben arbitrar procedimientos adecuados para modificar datos personales, de modo que el derecho de rectificación se activa cuando los datos son inexactos o incompletos.

c. Derecho de oposición

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho.

d. Derecho de cancelación

El artículo 32 de la Ley 534-2011 establece que los entes obligados serán responsables de proteger los datos personales y, en relación con estos, deberán adoptar procedimientos adecuados para recibir y responder las solicitudes de indagatoria, actualización, modificación y supresión de datos personales.

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho.

f. Derecho de consulta al registro general de protección de datos personales

El artículo 35 de la Ley 534-2011 señala que los entes obligados que posean, por cualquier título, registros o sistemas de datos personales, o que quieran suprimirlos deberán poner en conocimiento del Instituto de Acceso y Transparencia, una lista actualizada de los mismos y de la información general sobre sus protocolos de seguridad.

g. Derecho a indemnización por daños causados

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho. Sin embargo, el artículo 81 de la Ley 534-2011 determina la aplicación de sanciones sin perjuicio de las responsabilidades penales, civiles, administrativas o de otra índole en que incurra el responsable. Así, de suscitarse el caso y establecer responsabilidades, sobre todo de carácter civil, procederá a ordenarse las indemnizaciones que se consideraren pertinentes.

h. Derecho a la confidencialidad

La citada Ley 534-2011 señala, en el artículo 24, que se entiende por información confidencial, aquella referente al derecho a la intimidad personal y familiar, al honor y a la propia imagen, así como archivos médicos cuya divulgación constituiría una invasión a la privacidad de la persona; además, los datos personales que requieran el consentimiento de los individuos para su difusión. Aclara que los padres, madres y tutores tendrán derecho de acceso irrestricto a la información confidencial de los menores bajo su autoridad parental.

Como se desprende del texto, los datos personales son aquellos que en esencia tienen carácter de confidencial, tanto para garantizar el derecho a la intimidad y privacidad, como el derecho a la autodeterminación informativa, ya que en el literal a) se protege a estos en un contexto limitado a la intimidad, pero en el literal c) se menciona al consentimiento como elemento que permite el ejercicio del derecho a la protección de datos personales.

Llama la atención, la expresa mención del derecho de los padres a la información de sus representados, ya que de esta forma se identifica que niños y adolescentes no pueden ejercer por sí mismo sus derechos de intimidad, ni de protección de datos personales, cuando al acceder a herramientas tecnológicas de forma directa realizan el ejercicio de estos derechos. La única explicación sería que por el ámbito de la ley, se refiere exclusivamente a datos personales de menores en poder del Estado.

i. Derecho al olvido digital

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho.

j. Spam

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho.

h) Procedimiento

- *Solicitud:* El artículo 36 de la Ley 534-2011 dispone que los titulares de los datos personales o sus representantes, antes de la acreditación, podrán solicitar a los entes obligados, mediante la solicitud de información constante en el artículo 66 de la citada ley, esto es por solicitud dirigida al Oficial de Información, una solicitud en forma escrita, verbal, electrónica o por cualquier otro medio idóneo, de forma libre o en los formularios que apruebe el Instituto, lo siguiente: a. La información sobre la persona; b. Informe sobre la finalidad para la que se ha recabado tal información; c. La consulta directa de documentos, registros o archivos que contengan sus datos que obren en el registro o sistema bajo su control; d. La rectificación, actualización, confidencialidad o supresión de la información que le concierna, según sea el caso, y toda vez que el procedimiento para tales modificaciones no esté regulado por una ley especial.
- *Respuesta a la solicitud:* Tratándose de los literales a, b y c, los entes obligados deberán entregar, de forma gratuita conforme señala el artículo 37, en un plazo de diez días hábiles, contados a partir de la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente; o bien, le comunicarán por escrito que ese registro o sistema de datos personales no contiene los requeridos por el solicitante.
- *Plazo:* El Oficial de Información, entre cuyas funciones está la de recibir y dar trámite a las solicitudes referentes a datos personales a solicitud del titular y de acceso a la información (art. 50), deberá entregar al solicitante, en un plazo de treinta días hábiles desde la presentación de la solicitud, una comunicación sobre las modificaciones; o la razón por la cual no procedieron las reformas.
- *Recurso de apelación:* Contra la negativa de entrega de informes, o de la consulta directa, rectificación, actualización, confidencialidad o supresión de datos personales, procederá la interposición del recurso de apelación ante el Instituto, conforme el artículo 82. Asimismo, cuando la dependencia o entidad no entregue al solicitante los datos personales solicitados, o lo haga en un formato defectuoso o incomprensible; se niegue a efectuar modificaciones o correcciones a los datos personales; no esté conforme con el tiempo, el costo o la modalidad de entrega; la información entregada sea incompleta o no corresponda a la información requerida en la solicitud. También procederá dicho recurso en el caso de falta de respuesta en los plazos a que se refiere el artículo 36, esto es sobre informes finalidades, recursos en general, de conformidad con lo dispuesto en el artículo 38 de la Ley 534-2011.
- *Denegatoria del recurso de apelación:* Quedarán a salvo las demás acciones previstas por la ley, al tenor de lo dispuesto en el artículo 39 de la citada ley. Deberá presentarse el recurso por escrito, de forma libre o en los formularios que apruebe el Instituto. El Oficial de Información deberá remitir la petición y el expediente al Instituto a más tardar el siguiente día hábil de haberla recibido. Podrán interponerse además medidas cautelares, según el artículo 85 de la ley.
- *Subsanar deficiencias de derecho de las peticiones de los particulares:* El Instituto subsanará las deficiencias del recurso de apelación como de las denuncias y, únicamente si esto no fuere posible, requerirá al solicitante que subsane su escrito en un plazo de tres días hábiles (art. 85). Se admitirá el recurso en un término de tres días hábiles desde su presentación o de la subsanación por el recurrente o denunciante (art. 85).

- *Admisión del recurso o denuncia:* El Instituto lo someterá a uno de sus comisionados el caso de manera rotativa. El comisionado designado deberá, dentro de los quince días hábiles siguientes a la admisión del recurso o denuncia, dar trámite a la solicitud, formar el expediente, recabar pruebas y elaborar un proyecto de resolución que someterá al pleno del Instituto. Será comunicada al interesado y al ente obligado, el que deberá rendir informe dentro de un plazo de siete días hábiles a partir de la notificación. En caso de denuncia o si en el escrito de interposición del recurso se hiciere denuncia de una infracción por parte de un servidor público, este también será notificado inmediatamente y podrá justificar su actuación y alegar su defensa en el mismo plazo de siete días hábiles, al tenor de lo dispuesto en el artículo 88.
- *Prueba:* Las partes podrán ofrecer pruebas hasta el día de la celebración de la audiencia oral. Las pruebas aportadas en el proceso serán apreciadas según las reglas de la sana crítica (art. 90).
- *Audiencia oral:* El Instituto celebrará una audiencia oral con las partes en la cual conocerá la prueba, y el comisionado designado presentará el proyecto de resolución, conforme artículo 91.
- *Resoluciones:* Las resoluciones expedidas por el Instituto deberán ser fundamentadas en los hechos probados y las razones legales procedentes, bajo pena de nulidad, conforme el artículo 94.
- *Revocatoria:* Las partes podrán solicitar la revocatoria dentro del tercer día hábil de haberse notificado la resolución final, la cual deberá ser resuelta en los siguientes tres días hábiles, tal como señala el artículo 95.
- *Resoluciones definitivas:* El pleno resolverá, en definitiva, dentro de los tres días hábiles siguientes a la celebración de la audiencia. Las resoluciones del pleno serán públicas. Las resoluciones definitivas del Instituto podrán: a. Desestimar el recurso por improcedente o sobreseerlo. b. Confirmar la decisión impugnada del Oficial de Información. c. Confirmar la inexistencia de la información pública solicitada. d. Revocar o modificar las decisiones del Oficial de Información y ordenar a la dependencia o entidad que permita al particular el acceso a los datos personales, que reclasifique la información, o bien, que modifique tales datos. e. Establecer sanciones o requerir el trámite de imposición de las mismas a las autoridades respectivas. Las resoluciones deberán ser emitidas por escrito, establecerán los plazos para su cumplimiento y los procedimientos para asegurar su ejecución. La resolución definitiva que emita el Instituto tendrá fuerza ejecutiva (art. 96).
- *Improcedencia:* El recurso será desestimado por improcedente cuando: a. Sea incoado en forma extemporánea. b. El Instituto haya conocido anteriormente del mismo caso. c. Se recurra de una resolución que no haya sido emitida por el Oficial de Información, conforme el artículo 97.
- *Sobreseimiento:* El recurso será sobreseído cuando: a. El recurrente desista expresamente del mismo. b. El recurrente fallezca o, tratándose de personas jurídicas, se disuelvan. c. Admitido el recurso de apelación, aparezca alguna causal de improcedencia en los términos de la presente ley. d. La dependencia o entidad responsable del acto o resolución impugnada lo modifique o revoque, de tal manera que se extinga el objeto de la impugnación, conforme el artículo 98.
- *Silencio del Instituto:* Si el Instituto no hubiere resuelto el recurso de acceso a la información en el plazo establecido, la resolución que se recurrió se entenderá revocada por ministerio de ley, al tenor de lo que dispone el artículo 99.

- *Impugnación ante Sala de lo Contencioso Administrativo de la Corte Suprema de Justicia: Cuando* las resoluciones sean negativas a sus pretensiones. El procedimiento deberá respetar las garantías del debido proceso. Las actuaciones se sujetarán a los principios de legalidad, igualdad de las partes, economía, gratuidad, celeridad, eficacia y oficiosidad, entre otros. En lo referente al procedimiento, supletoriamente se sujetará a lo dispuesto por el derecho común, según lo dispuesto en los artículos 101 y 102.

i) Habeas data

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho.

a. Sujeto activo

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho.

b. Sujetos pasivos u obligados

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho.

c. Derechos tutelados por el habeas data

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho.

d. Procedencia del habeas data

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho.

e. Procedimiento del habeas data

No consta en la normativa constitucional ni legal salvadoreña referencia a este derecho.

j) Institucionalidad de protección

Con la aclaración de que la Ley 534-2011 tiene como ámbito de aplicación el público, la institución que elabora los formularios para solicitudes de acceso a la información, solicitudes referentes a datos personales y solicitudes para interponer el recurso de apelación (art. 58); establece los lineamientos para el manejo, mantenimiento, seguridad y protección de los datos personales y de la información pública, confidencial y reservada en posesión de las dependencias y entidades; por tanto el Instituto de Acceso a la Información Pública protege los datos personales en el sector público, el cual estará integrado por cinco comisionados y sus respectivos suplentes, quienes serán nombrados por el Presidente de la República, según el artículo 52 de la citada ley.

k) Régimen sancionador

Imputación de responsabilidad de servidor público: Si el Comisionado designado encontrare los elementos necesarios para atribuir a un servidor público la presunta comisión de una infracción, dentro de los tres días hábiles posteriores a su designación, lo remitirá al pleno del Instituto para que resuelva sobre la imputación dentro de un plazo no mayor de tres días hábiles. El servidor público dispondrá de siete días hábiles

contados a partir de la notificación para rendir su defensa, conforme el artículo 89. Cuando el Instituto determine durante la sustanciación del procedimiento que algún servidor público pudo haber incurrido en responsabilidad penal, deberá hacerlo del conocimiento del titular de la dependencia o entidad responsable y de la Fiscalía General de la República, en su caso, para que inicien el procedimiento de responsabilidad que corresponda. Asimismo, dará inicio el incidente sancionatorio ante el mismo Instituto (art. 100).

Impugnación por particulares en proceso contencioso administrativo: También podrá iniciarse el procedimiento de aplicación de sanciones mediante denuncia escrita de cualquier persona, en la cual se expondrá en detalle los hechos constitutivos de cualquiera de las sanciones e infracciones previstas en la presente ley y anexará las pruebas que tuviera en su poder, conforme el artículo 76.

Naturaleza de las infracciones: De conformidad con los artículos 76, 77, 78 y 79, las infracciones muy graves se refieren a la sustracción, destrucción, ocultamiento o cualquier tipo de daño o manejo inadecuado de la información que se encuentre bajo custodia o difusión de aquella con carácter de reservada o confidencial, o por la no entrega de información previamente ordenada por el Instituto.

Las infracciones graves son aquellas relativas a un actuar negligente respecto de la contestación a las solicitudes de acceso a la información o en la difusión de la información a que están obligados conforme a esta ley, o manejo inadecuado de información reservada.

Las infracciones leves se refieren a obstáculos para la entrega de información en su tiempo y debida forma.

l) Transferencia internacional de datos

No consta en la normativa constitucional ni legal panameña referencia a este tema.

m) Capacitación de los servidores públicos

Conforme el artículo 45 de la citada ley, se dispone que con la finalidad de promover una cultura de acceso a información en la administración pública, los entes obligados deban capacitar periódicamente a todos sus servidores públicos en materia del derecho de acceso a la información pública y el ejercicio del derecho a la protección de datos personales.

n) Promoción de cultura e inclusión en programas de estudio

Se ordena expresamente que el Ministerio de Educación incluya en los planes y programas de estudio de educación formal para los niveles inicial, parvulario, básico y medio, contenidos que versen sobre la importancia democratizadora de la transparencia, el derecho de acceso a la información pública, el derecho a la participación ciudadana para la toma de decisiones y el control de la gestión pública y el derecho a la protección de datos personales, al tenor de lo dispuesto en el artículo 46 de la ley analizada.

2.18 Jamaica

La Constitución de Jamaica, de 23 de julio de 1962, presentada ante el Parlamento, el 24 de julio de 1962,[1500] cuyo texto original está escrito en inglés señala, en el capítulo III sobre "Los derechos y libertades fundamentales" en el numeral 19, la protección de la privacidad del hogar y de la propiedad con el texto siguiente:

> 19. (1) Excepto con su propio consentimiento, ninguna persona estará sujeta a la búsqueda de su persona o su propiedad o a la entrada de otros en sus instalaciones. (2) Nada de lo contenido o hecho bajo la autoridad de ninguna ley se considerará inconsistente o contrario a esta sección en la medida en que la ley en cuestión contenga disposiciones razonablemente requeridas: **a.** en interés de la defensa, la seguridad pública, el orden público, la moralidad pública, la salud pública, los ingresos públicos, la planificación de la ciudad y el país o el desarrollo y la utilización de cualquier propiedad de manera que se promueva el beneficio público; **b.** permitir a cualquier persona jurídica establecida por cualquier ley para fines públicos o cualquier departamento del Gobierno de Jamaica o cualquier autoridad del gobierno local ingresar en las instalaciones de cualquier persona con el fin de realizar trabajos relacionados con cualquier propiedad o instalación que esté legalmente en tales locales y que pertenece a ese organismo corporativo o ese Gobierno o esa autoridad, según sea el caso; **c.** con el propósito de prevenir o detectar el crimen; o **d.** con el propósito de proteger los derechos o libertades de otras personas. [1501] (Traducido del inglés por la autora).

Una ley que desarrolle la *privacy* no ha sido dictada en Jamaica. Únicamente existe la Ley denominada *The Access to Informatio Act*, Ley 21-2002, H. F. COOKE, Governor-General, 22 de julio de 2002,[1502] cuyo contenido está relacionado con responsabilidad gubernamental, transparencia y participación pública en la toma de decisiones a nivel nacional hace referencia expresa a los documentos que afectan la privacidad de las personas en el artículo 22:

> 22.- (1) Sujeto a las disposiciones de esta sección, una autoridad pública no otorgará acceso a un documento oficial si al hacerlo esto implica la divulgación irrazonable de información relacionada con los asuntos personales de cualquier persona, ya sea viva o muerta. (2) La subsección (1) no se aplicará en los casos en que la solicitud de acceso tenga asuntos relacionados con el mencionado documento. (Traducido del inglés por la autora).

Se releva el sentido de racionalidad de la solicitud de acceso a información personal como garantía de la privacidad de los individuos que consta en el artículo 24 de la citada Ley 21-2002. Así como la posibilidad de solicitar información personal si está directamente relacionada con los documentos que se buscan (arts. 25, 26, 27 y 28, Ley 21-2002).

Aunque se desarrolla el texto como está construido, desde otro enfoque se analizará y verificará si el mismo contiene los criterios de análisis respecto de contenido esencial:

[1500] Order in Council, "Constitución de Jamaica de 1962", *Political Database of the Americas*, 1962, accedido 2 de febrero de 2018, http://pdba.georgetown.edu/Constitutions/Jamaica/jam62.html.
[1501] Ibíd.
[1502] Governor-General, "Ley No. 21-2002, The Access to Informatio Act", *OEA*, 2002, accedido 2 de febrero de 2018, http://www.oas.org/es/sla/ddi/docs/J2%20The%20Access%20to%20Information%20Act.pdf.

a) Ámbito: Registros o ficheros públicos y privados

El artículo 24, subnumeral 1, de la Constitución de Jamaica señala que el ámbito de aplicación de la ley es el público, al referirse a que debe ser documento oficial aquel del que se va a solicitar enmienda o anotación.

b) Naturaleza del dato

Conforme el artículo 3 de la Ley 21-2002 a objeto de interpretación se entiende por "documento" además de un documento por escrito: "(a) cualquier mapa, plan, gráfico o dibujo; (b) cualquier fotografía; (c) cualquier disco, cinta, pista de sonido u otro dispositivo en el que se incorporen sonidos u otros datos (que no sean imágenes visuales), ya sea electrónicamente o de otro modo, para reproducirse desde allí (con o sin la ayuda de otro equipo); (d) cualquier película (incluido microfilm), negativo, cinta u otro dispositivo en el que una o más imágenes visuales estén incorporadas, ya sea electrónicamente o de otro modo, para reproducirse desde allí (con o sin la ayuda de otro equipo)" (Traducido del inglés por la autora).

El numeral 19 de la Constitución de la República de Jamaica se trata de información relativa a la persona o a su propiedad.

c) Sujeto activo

De la redacción del numeral 19 de la Constitución de la República de Jamaica se entiende como titulares a las personas de quien se busca o se intenta obtener información, a la persona o a su propiedad.

d) Sujeto pasivo

No consta en la normativa constitucional ni legal jamaiquina referencia a este sujeto.

e) Objeto o bien jurídico

a. Derecho de información

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho. Por el contrario, el artículo 19 de la Constitución de Jamaica se refiere a *privacy*, a la cual le otorga un contenido no relativo únicamente a la información, sino directamente a la ubicación de la persona o su propiedad o a la entrada de otros en sus instalaciones.

b. Autodeterminación informativa

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

El artículo 19 de la Constitución de Jamaica determina en su numeral 2 que ante la ausencia de consentimiento por parte de su titular, ninguna persona estará sujeta a la búsqueda de su persona o su propiedad o la entrada de otros en sus instalaciones a menos que: la ley autorice a través de disposiciones razonablemente basadas en:

> **a.** en interés de la defensa, la seguridad pública, el orden público, la moralidad pública, la salud pública, los ingresos públicos, la planificación de la ciudad y el país o el desarrollo y la utilización de cualquier propiedad de manera que se promueva el beneficio público; **b.** permitir a cualquier persona jurídica establecida por cualquier ley para fines públicos o cualquier departamento del Gobierno de Jamaica o cualquier autoridad del gobierno local ingresar en las instalaciones de cualquier persona con el fin de realizar trabajos relacionados con cualquier propiedad o instalación que esté legalmente en tales locales y que pertenece a ese organismo corporativo o ese Gobierno o esa autoridad, según sea el caso; **c.** con el propósito de prevenir o detectar el crimen; o **d.** con el propósito de proteger los derechos o libertades de otras personas.[1503] (Traducido del inglés por la autora).

De la simple lectura de las autorizaciones expresamente señaladas en la Constitución se desprende que la posibilidad de limitar este derecho a la *privacy* está asociado a intereses generales, bien común y seguridad común.

d. Principios

i. Deber de información

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

ii. Pertinencia

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

iii. Calidad

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

iv. Finalidad

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

v. Seguridad

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

vi. Consentimiento

En el artículo 19 de la Constitución de Jamaica consta como piedra angular el consentimiento, ya que solo este autoriza a la búsqueda de una persona o de su propiedad o a la entrada de otros en sus instalaciones.

[1503] Order in Council, "Constitución de Jamaica de 1962".

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

a. Derecho de acceso

Conforme señala el artículo 30 (1) de la Ley 21-2002, el solicitante de acceso a un documento oficial puede, de conformidad con la subsección (4), solicitar una revisión interna de una decisión de una autoridad pública para: a) negarse a otorgar acceso al documento; (b) otorgar acceso solo a algunos de los documentos especificados en una aplicación; (c) aplazar la concesión de acceso al documento; (d) cobrar una tarifa por la acción tomada o en cuanto al monto de la tarifa.

b. Derecho de rectificación

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho. *Sin embargo, la* Ley 21-2002, al referirse a las enmiendas y anotación de registros personales en documentos oficiales, señala en el artículo 24 (1) que cuando una persona afirma que un documento oficial contiene información personal sobre la persona que: (a) es incompleto, incorrecto, desactualizado o engañoso la persona puede solicitar a la autoridad pública una enmienda o una anotación, según sea el caso, de ese documento; de tal manera que la información que constaría en el registro estaría completa, correcta, actualizada y no errónea con la ley.

Como se lee del citado artículo, los únicos criterios habilitantes para la modificación o anotación son la incompletitud, la incorrección, la desactualización y lo engañoso de la información que ha sido o puede ser utilizada por la autoridad pública; es decir, se requiere de dos condiciones para que opere este derecho.

c. Derecho de oposición

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

d. Derecho de cancelación

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

f. Derecho de consulta al registro general de protección de datos personales

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

g. Derecho a indemnización por daños causados

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

h. Derecho a la confidencialidad

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

i. Derecho al olvido digital

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

j. Spam

No consta en la normativa constitucional ni legal jamaiquina referencia a este derecho.

g) Procedimiento

El artículo 24 de la Ley 21-2002 determina que para solicitar una enmienda o una anotación de registros personales (art. 28), deberá presentarse por escrito, especificando, en la medida de lo posible, el documento que se reivindica, el registro personal que requiere enmienda o anotación, según sea el caso; así como especificando si la información en el registro se considera incompleta, incorrecta, desactualizada o engañosa, la base del solicitante para hacer ese reclamo; la naturaleza de la modificación requerida por el solicitante y la información que haría que el registro sea completo, correcto, actualizado y no erróneo con la ley.

Por su parte, los artículos 25, 26 y 27 regulan las actuaciones de la autoridad pública respecto de la petición de un interesado de realizar anotaciones de datos personales en actas o archivos oficiales. Si la autoridad está satisfecha con la verdad de los asuntos indicados en la solicitud modificará el documento y si no lo está no realizará la modificación. Pero aunque decida no enmendar un documento oficial, deberá tomar las medidas razonables para permitir que el solicitante proporcione su declaración la que contendrá la información que a su criterio haría el registro completo, correcto, actualizado y no engañoso. Si la autoridad ha modificado una anotación en un documento oficial así como si decide no hacerlo deberá tomar medidas razonables para informar al solicitante de la decisión y a otras autoridades que hayan hecho uso de dicho documento de la naturaleza de la enmienda o anotación y de los motivos de la decisión.

Posteriormente, conforme señala el artículo 30 (2) un solicitante de enmienda o anotación de un registro personal puede, de acuerdo con la subsección (4), solicitar una revisión de una decisión de una autoridad pública por negarse a hacer esa enmienda o anotación. La falta de decisión sobre cualquiera de los asuntos relativos al acceso de información personal, o para enmendar o anotar un registro personal dentro del tiempo requerido por esta ley, será considerado como una negativa a hacerlo.

El artículo 31 (1) de la citada ley señala que se realizará una revisión interna por el Ministro responsable en relación con los documentos o en cualquier otro caso, por el Secretario Permanente en el Ministerio correspondiente o el funcionario principal de la autoridad pública cuya decisión esté sujeta a revisión. La solicitud de revisión interna procede: (a) dentro de los treinta días posteriores a la fecha de notificación (en esta subsección denominada período inicial) al solicitante de la decisión pertinente, o dentro de dicho período adicional, que no exceda los treinta días, según lo permita la autoridad pública; o (b) cuando no se haya dado tal notificación, dentro de los treinta días

posteriores a la expiración del período permitido para la emisión de la decisión o de cualquier otro período permitido por la autoridad.

Respecto de la apelación, tal como determina el artículo 32, se realizará ante el tribunal establecido a tal efecto. Una persona puede presentar una apelación: (a) cuando la revisión interna de la sección 30 sea aplicable contra una decisión tomada en dicha revisión; si el tiempo de la revisión ha expirado sin que el solicitante haya sido notificado de una decisión; (b) en cualquier otro caso, contra una decisión relevante en relación con la negativa a realizar una modificación o anotación. La apelación se realizará: a) mediante la presentación de un documento en un plazo de sesenta días a partir de la fecha de notificación al recurrente de la decisión pertinente o de la decisión adoptada sobre un control interno; o cuando no se haya dado notificación dentro del período requerido por esta ley, dentro de los sesenta días posteriores a la expiración de dicho período. Cuando no se realiza una apelación dentro del período especificado, el Tribunal de Apelaciones puede extender ese período si está convencido de que la demora del apelante no es irrazonable.

La decisión sobre una apelación deberá ser tomada por el Tribunal de Apelaciones y su ejecución recaerá en la autoridad pública que tomó la decisión previa. Al escuchar una apelación, el Tribunal de Apelaciones puede tomar cualquier decisión que pueda haberse tomado en la solicitud original. Finalmente, el artículo 36 obliga al Ministro a que tan pronto como sea posible después del final de cada año (a más tardar el 30 de junio del año siguiente) prepare un informe del funcionamiento de esta ley durante el año, que contenga entre los asuntos especificados, el número de solicitudes recibidas de modificación de registros personales y de anotación de registros personales, así como las modificaciones y anotaciones realizadas.

h) Habeas data

No consta en la normativa constitucional ni legal jamaiquina referencia sobre el habeas data, ni como acción ni como procedimiento.

i) Institucionalidad de protección

No consta en la normativa constitucional ni legal jamaiquina referencia a este tema.

j) Régimen sancionador

No consta en la normativa constitucional ni legal jamaiquina referencia a este tema.

k) Transferencia internacional de datos

No consta en la normativa constitucional ni legal jamaiquina referencia a este tema.

2.19 Puerto Rico

La Constitución del Estado Libre Asociado de Puerto Rico de 1952 reconoce la *privacy* al tenor del texto siguiente: "**Sección 8.-** Toda persona tiene derecho a protección de ley contra ataques abusivos a su honra, a su reputación y a su vida privada o familiar"[1504].

Por eso, desarrolla el derecho a la *privacy* desde la perspectiva americana, en la Ley 111, 7 de septiembre de 2005, Ley de información al ciudadano sobre la seguridad y bancos de información,[1505] así como en la Ley 39-2012, Ley de Notificación Pública de Privacidad.[1506]

A continuación se incluirán únicamente aquellos criterios desarrollados en esta normativa específica a manera de ilustración, ya que no concierne construir el contenido esencial del derecho a la protección de datos personales debido al sesgo marcado por la *privacy*.

a) Ámbito: Registros o ficheros públicos y privados

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

b) Naturaleza del dato

Según la Ley 111-2005 para sus fines se entiende por "archivo de información personal" a un expediente que contenga al menos el nombre o primera inicial y el apellido paterno de una persona, combinado con cualquiera de los siguientes datos, de modo que se puedan asociar los unos con los otros y en el que la información sea legible sin necesidad de usar para acceder a ella una clave criptográfica especial: número de Seguro Social, número de licencia de conducir, tarjeta electoral u otra identificación oficial, números de cuentas bancarias o financieras de cualquier tipo, con o sin las claves de acceso que puedan habérsele asignado, nombres de usuario y claves de acceso a sistemas informáticos públicos o privados, información médica, información contributiva, evaluaciones laborales. No se incluye dentro de la información protegida la dirección postal o residencial ni información que sea documento público y esté disponible para la ciudadanía en general.

A efectos de la Ley 39-2012, Ley de Notificación Pública de Privacidad, se entiende por "información personal" cualquier nombre o número que pueda utilizarse, por sí mismo o junto con cualquier otra información, para identificar a un individuo en específico, incluyendo, pero sin limitarse: nombre y apellidos; número de seguro social; fecha y/o lugar de nacimiento; estado civil; género; dirección física o postal; código postal; dirección de correo electrónico; número de teléfono; número de licencia de conducir; número de pasaporte; huella(s) dactilar(es); grabaciones de voz; imágenes de retina; y

[1504] Convención Constituyente de Puerto Rico, "Constitución del Estado Libre Asociado de Puerto Rico de 1952", *Biblioteca Virtual Miguel de Cervantes*, accedido 28 de enero de 2018, http://www.cervantesvirtual.com/obra-visor/constitucion-del-estado-libre-asociado-de-puerto-rico-de-1952/html/8ce0e6e2-3815-4a73-8866-4cc9ecba835c_2.html#I_0_.

[1505] Asamblea Legislativa de Puerto Rico, "Ley No. 111, de 7 de septiembre de 2005, Ley de Información al Ciudadano sobre la Seguridad de Bancos de Información", *Sistema de Información de Prontuario de Leyes*, accedido 28 de enero de 2018, http://www.oslpr.org/prontuario/.

[1506] Asamblea Legislativa de Puerto Rico, "Ley Núm. 39-2012, Ley de Notificación Pública de Privacidad", *Sistema de Información de Prontuario de Leyes*, 2012, accedido 28 de enero de 2018, http://www.oslpr.org//files/docs/%7B1B4EE5A8-4E92-4FF3-A45E-9ABF0FB46322%7D.pdf.

cualquier otra información que permita identificar, física o electrónicamente, a una persona natural.

c) Sujeto activo

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

d) Sujeto pasivo

La Ley 39-2012, Ley de Notificación Pública de Privacidad, señala en el artículo 2 relativo a las definiciones el de *persona que recopila información personal*, que significa cualquier persona natural o jurídica que incurra en actividades comerciales dirigidas principalmente hacia la obtención de un beneficio mercantil o de remuneración monetaria y que en el curso de dichas actividades, por cualquier medio recopile y/o conserve información personal de residentes de Puerto Rico.

e) Objeto o bien jurídico

a. Derecho de información

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

b. Autodeterminación informativa

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho. Más bien queda claramente reconocido el derecho a la *privacy*.

c. Necesidad de mandato legal para tratamiento sin autorización del titular

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

d. Principios

i. Deber de información

De acuerdo con la Ley 39-2012, en el artículo 6 señala las normas generales sobre publicación de políticas de privacidad, esto es que todo Comercio incluirá en su página de internet un enlace en el cual el Consumidor pueda accesar y conocer su Política de Privacidad, acerca de la información personal de este, que el Comercio levante y/o conserve. (b) Toda política de privacidad deberá contener como mínimo lo siguiente: 1) Nombre del Comercio; 2) Que tipo de datos personales de los Consumidores estarán siendo recopilados por el Comercio; 3) Cuál es la política de divulgación de la Información Personal recopilada y bajo qué circunstancias será esta compartida con terceros; 4) Método disponible a los consumidores para que estos puedan conocer enmiendas realizadas a la Política de Privacidad de un Comercio, con posterioridad a la divulgación original de su Política Pública; 5) Fecha en que dichas enmiendas a la

política de privacidad entrarán en vigor; 6) Como la página de internet, responde a señales de "*Do Not Track*"; 7) Si terceros pueden recopilar información personal sobre las actividades en línea del consumidor, en diferentes páginas de internet; (c) El Comercio tendrá la opción de diseñar su propia política de privacidad basada en los criterios dispuestos en el artículo 6 (b), o podrá escoger de entre tres (3) categorías de protección de la Información Personal: nivel I, nivel III y nivel III, para denominar su Política de Privacidad; (d) Si el comercio u operador de página opta por utilizar uno de los tres modelos contenidos en los apéndices del reglamento, deberá cumplir con todos los criterios correspondientes a dicho modelo y utilizará el correspondiente logo.

ii. Pertinencia

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

iii. Calidad

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

iv. Finalidad

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

v. Seguridad

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

Únicamente, la Ley 111-2005 señala en el artículo 2 el concepto de "violación de la seguridad del sistema", que significa cualquier situación en que se detecte que se ha permitido el acceso de personas o entidades no autorizadas a los archivos de datos de modo que la seguridad, confidencialidad o integridad de la información en el banco de datos quede en entredicho; o cuando haya este acceso por personas o entidades normalmente autorizadas y se sepa o haya sospecha razonable que han violado la confidencialidad profesional u obtuvieron su autorización bajo falsas representaciones con la intención de hacer uso ilegal de la información. Incluye tanto el acceso a los bancos de información a través del sistema como el acceso físico a los medios de grabación que los contienen, y cualquier sustracción o movimiento indebido de dichas grabaciones.

Ante esas violaciones, el artículo 3 de la citada Ley 111-2005 establece que toda entidad propietaria o custodia de un banco de información para uso comercial, o toda entidad que dentro de sus funciones revenda o provea acceso a bancos de información digitales que incluya o contenga información personal de ciudadanos residentes en Puerto Rico, deberá notificar a dichos ciudadanos de cualquier violación de la seguridad del sistema y la misma no estuviera protegida con claves criptográficas más allá de una contraseña. La notificación a la clientela deberá hacerse de la manera más expedita posible, tomando en consideración la necesidad de las agencias del orden público de asegurar

posibles escenas de delito y pruebas, así como de la aplicación de medidas necesarias para restaurar la seguridad del sistema. Las partes responsables informarán dentro de un plazo improrrogable de diez (10) días de detectarse la violación de la seguridad del sistema al Departamento, el cual hará anuncio público al respecto dentro de veinticuatro (24) horas de recibir la información.

Por su parte, el artículo 4 de la Ley 111-2005 señala que la notificación de violación de la seguridad del sistema deberá indicar, hasta donde lo permitan las necesidades de cualquier investigación o caso judicial que se encuentre en curso, la naturaleza de la situación, el número de clientes potencialmente afectados, si se han radicado querellas criminales, qué medidas se está tomando al respecto y un estimado del tiempo y costo requerido para rectificar la situación. En el caso de que se sepa específicamente en qué se violó la confidencialidad de la información de un cliente identificable, dicho cliente tendrá derecho a conocer qué información quedó en entredicho. Para notificar a los ciudadanos, la entidad tendrá las siguientes opciones: 1. Notificación escrita directa a los afectados, por vía postal o por vía electrónica autenticada de acuerdo con la Ley de Firmas Digitales; 2. Cuando el costo de notificar a todos los potencialmente afectados de acuerdo al inciso (1) o de identificarlos sea excesivamente oneroso por la cantidad de personas afectadas, la dificultad en localizar a todas las personas, o la situación económica de la empresa o entidad; o siempre que el costo exceda los cien mil (100,000) dólares o el número de personas las cien mil, la entidad llevará a cabo su notificación mediante los siguientes dos pasos: a. Despliegue prominente de un anuncio al respecto en el local de la entidad, en la página electrónica de la entidad, si alguna, y dentro de cualquier volante informativo que publique y envíe a través de listas de correo tanto postales como electrónicas; b. Comunicación al respecto a los medios de prensa, que informe de la situación y provea información sobre cómo comunicarse con la entidad para darle mayor seguimiento. Cuando la información sea de relevancia en un sector profesional o comercial específico, se podrá efectuar este anuncio mediante las publicaciones o la programación orientada a ese sector de mayor circulación.

vi. Consentimiento

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

f) Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

a. Derecho de acceso

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

b. Derecho de rectificación

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

c. Derecho de oposición

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

d. Derecho de cancelación

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

e. Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

f. Derecho de consulta al registro general de protección de datos personales

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

g. Derecho a indemnización por daños causados

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

h. Derecho a la confidencialidad

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

l) Derecho al olvido digital

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

m) Spam

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

g) Procedimiento

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

Ahora bien, el artículo 7 de la Ley 39-2012 señala que el Secretario del Departamento de Asuntos del Consumidor (según el artículo 2) está facultado para requerir información a toda Persona que Recopile Información Personal. En caso de rebeldía o negativa a obedecer una citación expedida por el Secretario o cualquier funcionario designado por este, cualquier sala del Tribunal General de Justicia podrá, a solicitud del Secretario, expedir una orden contra dicha persona, requiriéndole comparecer ante el

Secretario o ante el funcionario designado por este, para presentar evidencia si así se ordenare o para declarar sobre el asunto bajo investigación. Dicha persona incurrirá en desacato si desobedeciere la orden del tribunal.

h) Habeas data

No consta en la normativa constitucional ni legal referencia a este derecho.

a. Sujeto activo

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

b. Sujetos pasivos u obligados

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

c. Derechos tutelados por el habeas data

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

d. Procedencia del habeas data

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

e. Procedimiento del habeas data

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

i) Institucionalidad de protección

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

El artículo 7 de la ley citada, respecto de los requerimientos de información e investigación, señala que es el Secretario del Departamento de Asuntos del Consumidor (según el artículo 2), el que está facultado para, en el ejercicio de sus deberes, requerir información a toda Persona que Recopile Información Personal. Esto incluye pero no se limita a cursar requerimientos de información, citar testigos, tomar juramentos y declaraciones. En cumplimiento de estas disposiciones, podrá extender citaciones bajo apercibimiento y obligar la comparecencia de testigos. Además, como parte de sus facultades podrá requerir que se le presenten libras, cartas, documentos, recibos, expedientes, fotos y cualquier otro artículo que considere esencial para establecer que el investigado en efecto ha cumplido con su obligación en ley, de publicar su Política de Privacidad.

j) Régimen sancionador

La Ley 111-2005 establece en el artículo 8 que será el Secretario del Departamento de Asuntos del Consumidor (según el artículo 2), quien podrá imponer multas desde quinientos (500) dólares hasta un máximo de cinco mil (5,000) dólares por cada violación a las disposiciones de esta ley o de su reglamento relativas a las notificaciones de violaciones de seguridad a los titulares de los datos personales. Las multas dispuestas en este artículo no afectan los derechos de los consumidores de iniciar acciones o reclamaciones en daños ante un tribunal competente.

Por su parte, la Ley 39-2012 señala en el artículo 8, relativo a las penalidades, que en caso de que un Operador de Páginas o una Persona que Recopila Información Personal incurra en la práctica de divulgar una Política de Privacidad que no corresponda a la realidad de sus prácticas de manejo de información personal; o incurra en la práctica de divulgar un símbolo, o logo, no autorizado; o que no corresponda a la realidad de sus prácticas de manejo de información personal, se incurrirá en una infracción administrativa que estará sujeta a una multa de hasta un máximo de cincuenta mil dólares ($50,000). Cualquier otra violación a lo dispuesto por este Reglamento estará sujeta a multas administrativas de hasta diez mil dólares ($10,000.00) por cada ocurrencia. Se considerara que se configura una ocurrencia separada y distinta por cada día en que un Comercio no cumpla con su obligación de divulgar una Política de Privacidad en debida forma.

k) Transferencia internacional de datos

No consta en la normativa constitucional ni legal puertorriqueña referencia a este derecho.

2.20 Cuba

La Constitución Política de la República de Cuba, que incluye reformas de 1978, 1992 y 2002, no menciona referencia alguna a derechos de intimidad, privacidad o protección de datos personales o a los abusos que pueden producirse por el uso de las tecnologías de la información y comunicación. A lo sumo, determina en el artículo 56 la inviolabilidad del domicilio y en el artículo 57, la inviolabilidad de la correspondencia. Tampoco existe referencia respecto del derecho a la libertad informática, ni el derecho de acceso a la información.

Según Ojeda y Amoroso, en vista de que Cuba carece de normativa constitucional y legal específica y por ello la "necesidad de ampliar las formas de asegurar el ya mencionado principio dignidad humana, pues en tanto sea inexistente la regulación expresa, en el ámbito constitucional, del derecho a la protección de datos personales, los conflictos que se generen continuarán sin una vía de solución adecuada y el restablecimiento del daño causado será nulo"[1507].

A continuación se enumerarán varias normas de carácter sectorial que mencionan de alguna manera una forma de protección de la información o de los datos personales:

[1507] Z. OJEDA Y Y. AMOROSO, "La protección de los datos personales en Cuba desde la legislación vigente", *Justicia Juris*, vol. 12, 2 (2016), 87-94, accedido 28 de enero de 2018, http://www.scielo.org.co/pdf/jusju/v12n2/1692-8571-jusju-12-02-00087.pdf.

- Para datos de carácter crediticio la norma aplicable es la Resolución 66/1998, del 1 de junio de 1998, sobre el Reglamento sobre el Secreto Bancario,[1508] que establece que deberá observarse reserva sobre los datos relativos a las fuentes, el destino, la cuantía, los nombres de los interesados, el nombre de los titulares de las cuentas, los saldos, entre otros, es decir la protección de los datos patrimoniales de las personas.
- Decreto Ley 199/ 1999, promulgado el 2 de diciembre de 1999, sobre la Seguridad y Protección de la Información Oficial Cuba.[1509]
- La Resolución 85 de 2004, del Ministerio de la Informática y las Comunicaciones, que regula el funcionamiento de las entidades cubanas que brindan los Servicios de Navegación por Internet y/o Correo Electrónico Nacional e Internacional.[1510]
- La Resolución ministerial 1/2007, 9 de enero de 2007, determina el Reglamento General de Hospitales de Cuba,[1511] que se refiere a datos de salud en las historias clínicas.
- La Resolución 127, 24 de julio de 2007, con la cual se pone en vigencia el Reglamento de Seguridad para las Tecnologías de la Información.[1512]
- El Decreto-Ley 281/2012, promulgado el 8 de febrero del 2012, sobre el Sistema de Información del Gobierno.[1513]

2.21 Haití

En la Constitución de la República de Haití[1514] la única referencia es el artículo 40, referido a la información pública y al derecho de los ciudadanos de conocerla, al tenor del texto siguiente:

[1508] Ministro - Presidente del Banco Central de Cuba, "Resolución 66/1998, Reglamento sobre el Secreto Bancario. La Habana, Cuba", *Banco Central de Cuba*, accedido 28 de enero de 2018, http://www.bc.gob.cu/Manual/Cap%C3%ADtulo%2010.%20Regulaciones%20generales/10.02%20-%20Resoluci%C3%B3n%20No.%2066%20de%201ro.%20de%20junio%20de%201998.%20Reglamento%20sobre%20el%20Secreto%20Bancario.pdf.

[1509] Consejo de Estado de la República de Cuba, "Decreto Ley No. 199 de 25 de noviembre de 1999 Sobre la Seguridad y protección de la Información Oficial. Gaceta Ordinaria-78-1999 de 02/12/1999", *Gaceta Oficial de la República de Cuba*, accedido 28 de enero de 2018, https://www.gacetaoficial.gob.cu/codbuscadores.php.

[1510] Ministerio de la Informática y las Comunicaciones de Cuba, "Resolución No. 85 de 2004 que regula el funcionamiento de las entidades cubanas que brindan los Servicios de Navegación por Internet y/o Correo Electrónico Nacional e Internacional", accedido 28 de enero de 2018, http://www.fcmjtrigo.sld.cu/resoluciones/resol_85_2004.pdf.

[1511] Ministerio de Salud Pública de Cuba, "Resolución Ministerial No 1/2007", *Legislación para el Sistema Nacional de Salud*, accedido 28 de enero de 2018, http://legislacion.sld.cu/index.php?P=FullRecord&ID=151.

[1512] Ministerio de la Informática y las Telecomunicaciones de Cuba, "Resolución No. 127 del 2007 del 24 de julio de 2007, Reglamento de Seguridad para las Tecnologías de la Información", *Ministerio de la Informática y las Telecomunicaciones*, accedido 28 enero 2018, en http://www.poljgrave.sld.cu/download/R%20127-07.pdf.

[1513] Consejo de Estado de la República de Cuba, "Decreto-Ley 281/2012, promulgado el 8 de febrero del 2012. Sistema de Información del Gobierno", *Gaceta Oficial de la República de Cuba*, p. 29, accedido 28 de enero de 2018, https://www.gacetaoficial.gob.cu/codbuscadores.php.

[1514] Asamblea Nacional Constituyente, "Constitución de la República de Haití de 1987", *Political Database of the Americas*, 1987, accedido 28 de enero de 2018, http://pdba.georgetown.edu/Constitutions/Haiti/haiti1987fr.html.

> Sección I. Derecho a la información. Artículo 40: El Estado está obligado a dar publicidad, a través de una prensa, escrita y televisada, en criollo y en francés, a las leyes, decretos, decretos, acuerdos internacionales, tratados, convenciones, a todo lo que concierne a la vida nacional, con excepción para información relacionada con la seguridad nacional.[1515] (Traducido del francés por la autora).

No existe normativa específica que desarrolle el derecho a la protección de datos personales.

3. Formas de reconocimiento del derecho a la protección de datos personales en Latinoamérica

Luego de la revisión realizada de la normativa de cada uno de los países latinoamericanos se puede realizar arribar a una primera conclusión, esto es que existe heterogeneidad en las formas de reconocimiento del derecho a la protección de datos personales en la región.

De manera general, la respuesta latinoamericana a la tendencia mundial de proteger a las personas de las transgresiones producidas por la tecnología y la informática aparecieron de forma cronológica mediante:

a) *Protección de los datos personales a través de* ***otros derechos relacionados*** *(intimidad o privacidad)*, por medio de normas constitucionales:

   Aunque la mayoría de los países tuvieron un desarrollo paulatino, es decir el primigenio reconocimiento de la intimidad y la privacidad para luego decantarse por el derecho a la protección de datos personales. Sin embargo, actualmente subsisten países en los que no se ha superado esta visión y en los que las Constituciones no reconocen ni el derecho ni la garantía de *habeas data.* Por ejemplo: se abrogó la Constitución Boliviana que contenía esta acción y aprobó la denominada acción de protección de la privacidad, que el tribunal constitucional interpreta como idéntica al *habeas data*, pero que al parecer su contenido se limita exclusivamente a la intimidad y/o la privacidad y no a otros derechos que permiten el libre desarrollo de la personalidad a través de los datos de una persona, como el derecho a la protección de datos personales.

   Asimismo, Chile solo reconoce a nivel constitucional el derecho a la vida privada y promulga una ley que pese a sus varias reformas sigue anclada a la privacidad (1999, 2002, 2011 y 2012); actualmente se encuentra en proceso de aprobación una reforma constitucional que incluya el derecho a la protección de datos personales, aún en trámite (2019).

   Por su parte, Paraguay (1992) y Venezuela (1999) si bien reconocen nominalmente la garantía constitucional de *habeas data* el contenido de estas garantías constitucionales se centran en la protección de la intimidad y la privacidad. En el caso de Honduras, su Constitución (2003 y 2006) incorpora al *habeas data* pero asociado únicamente al derecho a la intimidad sin mencionar la privacidad. Ninguno de estos países reconoce a nivel constitucional ni legal el

[1515] Ibíd.

derecho a la protección de datos personales y tampoco desarrolla normativa legal al respecto. Se aclara que el caso de Paraguay, existe la Ley 1682, 16 de enero de 2001, que protege los datos personales, únicamente, en bases de datos del sector privado.

En cuanto a Guatemala (1985), se protegen los datos personales desde una perspectiva limitada, ya que el ámbito de aplicación de esta norma es el Estado, a quien se considera el único responsable de tratamiento de datos personales, excluyendo de esta forma a los responsables privados. Ahora bien, la Corte de Constitucionalidad de Guatemala (2006) garantiza los datos personales contenidos en ficheros regentados por entes privados desde otros derechos fundamentales como la intimidad personal, la privacidad y el honor.

b) *Reconocimiento de la garantía constitucional denominada **habeas data***:

Tal es el caso de Brasil (1988), Paraguay (1992), Perú (1993), Ecuador (1996), Venezuela (1999), Panamá (2002), Honduras (2003), República Dominicana (2010) y Nicaragua (2014). Estos países consagran el *habeas data* como garantía constitucional abierta, es decir a través de éste se tutelan varios derechos, entre ellos la protección de datos personales: que incluye los derechos de autodeterminación informativa: acceso, rectificación, eliminación y oposición; así como de otros derechos subjetivos que también pueden sufrir afecciones por un uso inadecuado de los datos de sus titulares como son: la intimidad, la privacidad, el honor, la imagen, la propia voz, la identidad, entre otros.

c) *Acciones constitucionales tradicionales como **la tutela** y el **amparo** que incluyen en ellas al contenido del habeas data*.

Como ocurre en el caso de Colombia (1991) mediante la acción de tutela. De Argentina a través de la acción de amparo (1994). De México por medio de la Ley de Amparo, reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos, cuyas últimas modificaciones corresponden al 17 de junio de 2016 que regulan el Juicio de Amparo que procede sobre derechos constitucionales como el de protección de datos personales (art. 16 de la Constitución citada). Finalmente, de Bolivia, que incorpora la acción denominada de protección de la privacidad, aunque como vimos con claras limitaciones a su tutela, ya que el inadecuado manejo de los datos debe primeramente afectar la intimidad y la privacidad.

d) *Reconocimiento del **derecho a la protección de datos personales** como derecho constitucional.*

Este es el caso de: Colombia (1991), Perú (1993), Panamá (2002), Ecuador (2008), Nicaragua (2014), México (2009), República Dominicana (2010) y Chile (se encuentra en proceso de aprobación, 2018).

En el caso de Ecuador, si bien existe reconocimiento constitucional del derecho, no se ha dictado normativa que lo desarrolle.

Respecto a Costa Rica y El Salvador, no aparece en su norma constitucional referencia al *habeas data* ni tampoco norma que reconozca el derecho, sino que en estos países el derecho a la protección de datos personales se incorpora por vía jurisprudencial.

Costa Rica lo hace mediante las sentencias 4154-97, 7175-97, 4347-99 y 5802-99, reconociendo el citado derecho. Lo mismo ocurre con El Salvador, que por medio de precedentes jurisprudenciales dictados por la Corte Suprema de Justicia, al tenor de las resoluciones de amparo 118-2002, acción de inconstitucionalidad 36-2004 y de amparo 934-2007 incorpora este derecho.

Finalmente, la Constitución de Uruguay no excluye de la enumeración de derechos, deberes y garantías a otros derechos que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno. En consecuencia, es posible invocar el derecho a la protección de datos personales, y este es el fundamento de la ley específica dictada en la materia en dicho país.

e) *Normativa legal e incluso reglamentaria específica y especializada que desarrolla el derecho constitucional a la protección de datos personales*

Este es el caso de países como: Perú (2004), México (2010 y 2017), Colombia (2012), Nicaragua (2012), República Dominicana (2013) y Panamá (2019).

f) *Normativa legal e incluso reglamentaria específica y especializada que desarrolla la garantía constitucional de habeas data:*

Este es el caso de naciones como: Perú (2004), México (2010 y 2017), Colombia (2012), Nicaragua (2012) y República Dominicana (2013), Brasil (2019) y Panamá (2019). En Latinoamérica suele ocurrir que el país que tiene reconocido el derecho constitucional también tiene la garantía de *habeas data* o alguna de las otras acciones equivalentes, y que más bien lo tardío ha sido la emisión de la normativa legal aplicable.

g) Normativa legal e incluso reglamentaria específica y especializa que desarrolla el derecho a la protección de datos personales, aun cuando no cuente con reconocimiento constitucional:

Como es el caso de: Argentina (2000), Costa Rica (2011) y Uruguay (2008).

h) *Normativa dispersa de carácter sectorial*

Como es el caso de Bolivia, Ecuador, Honduras, El Salvador, Guatemala y Cuba. Y los casos especiales de Paraguay, cuya Ley 1682, 16 de enero de 2001, se limita a regular información en bases de datos de carácter privado; y Chile, que por una cuestión de índole histórico-social evita reformas constitucionales y prefiere dictar leyes, por lo que al respecto ha dictado la Ley 19.628 en 1999 que desarrolla únicamente la vida privada.

i) *Reconocimiento de otras formas de protección como The privacy*.

Este es el caso de Jamaica y de Puerto Rico. Jamaica reconoce el derecho a la *Protection for privacy of home and other property*, en la Constitución de Jamaica de 23 de julio de 1962.[1516] Puerto Rico consagra, en la sección 8 de su Constitución,[1517] el derecho a la protección de la ley contra ataques abusivos a la honra, reputación y a la vida privada o familiar de la persona. Sin embargo, desarrolla estos derechos desde la perspectiva americana, como se evidencia del contenido de la Ley 111, 7 de septiembre de 2005, Ley de información al ciudadano sobre la seguridad y bancos de información,[1518] y de la Ley 39-2012, Ley de Notificación Pública de Privacidad.[1519]

j) *Ausencia de normativa relacionada y específica*.

Como el caso de Haití, que carece de normativa constitucional y legal.

De lo visto, la figura del *habeas data* en Latinoamérica es fundamental para el desarrollo del derecho a la protección de datos personales en la región.

El *habeas data* nace en Brasil (1988), Paraguay (1992), Perú (1993), Ecuador (1996), Venezuela (1999), Panamá (2002), Honduras (2003), República Dominicana (2010) y Nicaragua (2014) como garantía constitucional para proteger a las personas de las posibles afectaciones que pudieran producirse por el uso inadecuado de sus datos personales a través de tecnologías de la información y comunicación.

Si bien el *habeas data* fue concebido como acción procesal, el momento de la redacción de los textos constitucionales, se señala que a través de éste se pueden ejercer derechos como el de acceso, rectificación, eliminación, entre otros. Por lo que, varios países latinoamericanos que no reconocen a la protección de datos personales como derecho fundamental entienden que el *habeas data* es al mismo tiempo derecho y garantía (Argentina, Brasil, Paraguay, Venezuela, Honduras y Bolivia)[1520]. En este sentido, podemos decir que, en Latinoamérica, la protección de datos personales, reconocido como derecho fundamental, tiene su origen directo en la garantía constitucional del *habeas data*.

De otro lado, aquellas naciones que incorporaron a la protección de datos personales como derecho constitucional[1521] y que además consagran el *habeas data*[1522] o sus

[1516] Order in Council, "Constitución de Jamaica de 1962".
[1517] Convención Constituyente de Puerto Rico, "Constitución del Estado Libre Asociado de Puerto Rico de 1952", cit.
[1518] Asamblea Legislativa de Puerto Rico, "Ley No. 111, de 7 de septiembre de 2005, Ley de Información al Ciudadano sobre la Seguridad de Bancos de Información".
[1519] Asamblea Legislativa de Puerto Rico, "Ley No. 39-2012, Ley de Notificación Pública de Privacidad".
[1520] Anotándose que, en los casos de Honduras y Venezuela, lamentablemente, el texto constitucional, limita el ámbito de protección del *habeas data* a la intimidad y la privacidad. En el caso Boliviano, existe un desarrollo jurisprudencial que debe seguir evolucionado, de tal forma que a través de la acción de protección de la privacidad se pueda proteger todo tipo de datos y no solo aquellos considerados íntimos.
[1521] Colombia (1991), Perú (1993), Panamá (2002), Ecuador (2008), Nicaragua (2014), México (2009) y República Dominicana (2010)
[1522] Brasil (1988), Paraguay (1992), Perú (1993), Ecuador (1996), Venezuela (1999), Panamá (2002), Honduras (2003) República Dominicana (2010) y Nicaragua (2014).

equivalentes, como mecanismos de tutela[1523], gozan de un mayor nivel de protección, ya que, la clara diferenciación entre derecho y garantía repercute positivamente en la delimitación conceptual de ambas instituciones.

Esta adecuada ubicación de conceptos ha permitido ampliar el alcance del *habeas data*, pues no se restringe a la protección de un único derecho sino que puede tener un múltiple factor de protección, es decir a través de esta herramienta constitucional se pueden tutelar varios derechos fundamentales como: el de la intimidad, la privacidad, la imagen, la propia voz, la identidad, la igualdad, la autodeterminación informativa, la protección de datos de carácter personal, entre otros. Cada uno de estos derechos pueden tener manifestación digital, es decir pudieran ser transgredidos, incluso simultáneamente, por un inadecuado tratamiento de los datos personales. En este sentido, la garantía constitucional se vuelve integral pues permite proteger a la persona, en sus distintas interrelaciones con la tecnología, en su autodeterminación informativa o en el ejercicio de sus libertades individuales en los espacios digitales.

Igualmente, está clara diferenciación entre derecho y acción procesal constitucional ha permitido delinear de mejor manera el contenido esencial del derecho a la protección de datos personales y diferenciarlo de los otros derechos fundamentales que permiten el desarrollo de la personalidad de un individuo.

En conclusión, en la región se presentan dos modelos, uno, en el que el habeas data representa en sí mismo el reconocimiento al derecho a la protección de datos personales y otro en el que, es herramienta de protección de éste y otros derechos de la personalidad.

Finalmente, aunque es evidente la heterogeneidad de la forma de abordar la protección de los datos personales de los países latinoamericanos, el actual desarrollo de la sociedad ha permitido que el derecho a la protección de datos se incorpore en la normativa constitucional, legal o jurisprudencial, como veremos a detalle en el siguiente capítulo.

[1523] Colombia (1991), acción de tutela. Argentina (1994), acción de amparo. México (2016), acción de amparo, Bolivia (2009), acción de protección de la privacidad.

CAPITULO V

CONTENIDO ESENCIAL DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN LATINOAMÉRICA

1. El contenido esencial del derecho a la protección de datos personales en Latinoamérica

Conforme el objetivo de la presente investigación, es menester identificar, analizar y colegir aquellos elementos que conforman el contenido esencial del derecho a la protección de datos personales desde la perspectiva latinoamericana. Como la región tiene sus particularidades, además del análisis en aquellos países en los cuales existe reconocimiento constitucional del derecho, es necesario analizar la garantía procesal del *habeas data* o su equivalente como parte fundamental de este sistema de protección específico.

La garantía constitucional del contenido esencial está presente en la normativa latinoamericana, con la finalidad de limitar al poder y buscar el respeto de la naturaleza nuclear o central de cada derecho o libertad fundamental. Pero además, y a efectos de la presente investigación, permite determinar la sustancia del derecho.[1524]

Para cumplir con esa finalidad, en líneas precedentes se analizó la normativa constitucional y legal de los países más representativos de América Latina. Para lo cual se identificaron aquellos presupuestos indispensables para establecer el contenido esencial de un derecho, estos son: ámbito: registros o ficheros públicos y privados; naturaleza del dato; sujeto activo; sujeto pasivo; objeto o bien jurídico: derecho de información, autodeterminación informativa, necesidad de mandato legal para tratamiento sin autorización del titular; principios: deber de información, pertinencia, c*alidad, finalidad, seguridad, consentimiento; c*ontenido de las facultades que les corresponden a los titulares para el ejercicio del objeto: derecho de acceso, derecho de rectificación, derecho de oposición, derecho de cancelación, derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales, derecho de consulta al registro general de protección de datos personales, derecho a indemnización por daños causados, derecho a la confidencialidad, derecho al olvido digital, spam, procedimiento; *habeas data* o similares: s*ujeto activo*, sujetos pasivos u obligados, derechos tutelados por el *habeas data*, procedencia del *habeas data*, procedimiento del *habeas data*; institucionalidad de protección; régimen sancionador; transferencia internacional de datos y características propias de cada legislación.

Como son varios países que integran la región, es necesario agruparlos según niveles de protección del derecho; de modo que el análisis se pueda dividir entre aquellos cuyo contenido esencial se asimila al modelo europeo. Es decir, aquellos que además del

---

Presidencia de la República Oriental del Uruguay, "Decreto N° 414/009, de 31 agosto de 2009, Reglamenta la Ley de Protección de Datos Personales", *Agesic*, 2009, accedido 25 de agosto de 2017, https://www.agesic.gub.uy/innovaportal/v/295/1/agesic/decreto-n%C2%B0-414_009-de-31-agosto-de-2009.html.

[1524] E. ÁLVAREZ CONDE, *Curso de Derecho constitucional*, vol. 1, 1, (Madrid: Tecnos, 2008), 641.

reconocimiento de la protección de datos personales como un derecho fundamental, el reconocimiento de un sistema de garantías constitucionales, ha consagrado normativa legal específica que permite la materialización de la autodeterminación informativa. De aquellas naciones cuyo reconocimiento es limitado a la normativa constitucional sustentada en el *habeas data* como garantía constitucional sin normativa legal que desarrolle el derecho o cuya normativa es anticuada, insuficiente, sectorial o anidada en la intimidad, es decir aquellos que no alcanzan un estándar europeo de protección.

No serán parte del análisis del contenido esencial aquellos países latinoamericanos que contemplan otras formas o mecanismos de protección, como los aplicados por el modelo norteamericano basado en *the right of privacy*, como son *Jamaica y Puerto Rico*.

Asimismo, se excluirán de este análisis a aquellos países que no han desarrollado normativa constitucional ni legal de aplicación general que permita determinar el contenido esencial del derecho, que solo ha dictado normativa secundaria de carácter sectorial como Cuba, o como el caso de Haití, que en su Constitución únicamente menciona el derecho de acceso a la información pública.

Desde esa perspectiva, se establecerá un panorama general que permita identificar elementos comunes que puedan ser incluso innovadores en el sistema de protección; así como, discutir los argumentos fácticos y jurídicos de aquellos sistemas, reglas, principios y derechos que debieran perfeccionarse, incorporarse, reformarse o eliminarse para constituir un sistema latinoamericano coherente de protección.

1.1 Ámbito: Registros o ficheros públicos

Como se analizó previamente, no todos los países reconocen el derecho fundamental a la protección de datos personales, sino que varios aún se aferran a la intimidad o a la privacidad. Sin embargo, aun en estos casos se colige que es fundamental en la configuración del contenido esencial una dimensión completa, es decir, un ámbito de protección tanto en lo público como en lo privado, pues la protección debe ser integral, de tal manera que la aplicación sea general, uniforme, en todas las esferas en las que se desenvuelve una persona, pues solo de esta manera es posible el ejercicio pleno de un derecho en sociedad.

A continuación, desde las distintas formas de salvaguarda de los datos personales se puede colegir los siguientes criterios de análisis:

a) *Se reconoce en el ámbito público y privado el derecho a la protección de datos personales*

Brasil, el artículo 1 y 3 de la Ley LGPD, 13,709/18 prevé el procesamiento de datos personales en medios físicos y digitales, por parte de una persona jurídica y natural de derecho público o privado, independientemente del medio, del país de su sede o del país donde estén localizados los datos. Con esta normativa se supera la visión inicial del artículo 5 de la Constitución de la República Federativa del Brasil de 1988, que señala que el único ámbito aplicable del *habeas data*, aferrado al derecho a la intimidad, eran los ficheros públicos. Asimismo, la nueva Ley de Protección de Datos Personales amplía la visión limitada del Marco Civil Brasileño de Internet promulgado en el 2014

consagra a favor de las personas naturales, el ejercicio del derecho a la protección de datos personales, pero respecto únicamente de los responsables de transmisión, conmutación o ruteo; es decir, en un limitado ámbito privado.

Colombia, en el artículo 2 de la Ley 1266 de 2008, que regula el *habeas data* consta expresamente que el ámbito de aplicación son las bases públicas y privadas.

Perú, la Constitución del Perú de 1993, tanto en el reconocimiento del derecho como del *habeas data* determinan que el ámbito de aplicación del derecho a la protección de datos personales son los ficheros públicos y privados.

Argentina, el artículo 1 de la Ley 25.326 de 2000, de Protección de Datos Personales, tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos o privados.

Ecuador, mediante la acción de *habeas data* que procede para proteger no solo intimidad, buen nombre, honor, imagen y propia voz, sino protección de datos personales se protege los datos personales que consten en entidades públicas o privadas, Constitución del Ecuador de 2008.

Nicaragua, desde 1995 protege ficheros públicos, pero desde 2014 también incluye ficheros privados, conforme la Ley 854, Ley de Reforma Parcial a la Constitución Política de la República de Nicaragua, 29 de enero de 2014, Publicado en la Gaceta 26, 10 de febrero de 2014.

Uruguay, la Ley 18.331/2008 y el Decreto 414/2009 determinan la aplicabilidad de la regulación que protege los datos personales, tanto en bases de datos públicas como privadas.

Costa Rica, la Ley 8968/2011, relativa al ámbito de aplicación de la ley, protege datos personales que se encuentran en bases de datos automatizadas o manuales incluidas modalidades de uso posterior de datos, tanto de organismos públicos como privados.

El Salvador, la Ley 534-2011, Ley de Acceso a la Información Pública de El Salvador, refiere a las finalidades de la ley; señala entre ellas la de proteger los datos personales en posesión de los entes obligados, estos son de carácter público. Sin embargo, mediante la jurisprudencia se incorpora protección a bases de datos en manos de entes privados, resoluciones de amparo 118-2002, acción de inconstitucionalidad 36-2004 y de amparo 934-2007.

México, protege los ámbitos públicos y privados con leyes especializadas. La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de 2017 protege los datos personales en bases de datos públicas, mientras que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de 2010, precautela datos personales en bases de datos privadas.

Panamá, el artículo 1 de la Ley 81, de Protección de Datos Personales de Panamá, señala que toda persona, natural o jurídica, de derecho público o privado, lucrativa o no,

puede efectuar el tratamiento de datos personales, siempre que lo haga con arreglo a la presente Ley y para los fines permitidos en el ordenamiento jurídico. Lo que coincide con lo dispuesto en el artículo 42 de la Constitución de 2002 que señala que las personas tienen derecho de acceder a datos personales en bases de datos que son de carácter público y privado. Con la citada Ley, se supera la limitación constante en el artículo 44 de la misma norma constitucional que determina que solo se podrá promover la acción de *habeas data* cuando los datos han sido recabados en bancos de datos o registros oficiales o particulares, siempre que se trate de empresas que prestan un servicio al público o se dediquen a suministrar información, puesto que la nueva ley estipula un ámbito de protección amplio sin condiciones.

b) Se reconoce el ámbito público y privado, mediante habeas data anclado en la intimidad y la privacidad

Honduras, el artículo 182 de la Constitución de Honduras de 1982, reformada en 2003 y 2006, expresamente señala que el *habeas data* solo puede promover la persona cuyos datos personales o familiares consten en medios convencionales, electrónicos o informáticos, en cualquier archivo o registro, privado o público.

Venezuela, en el artículo 28 de la Constitución determina que el *habeas data* puede ejercitarse respecto de datos que consten en registros oficiales o privados, con las excepciones que establezca la ley.

c) Se reconoce el ámbito público y privado, únicamente mediante privacidad o la intimidad

Bolivia, el artículo 130 de la Constitución de 2009 señala que el ámbito de aplicación de la acción de protección de privacidad son los archivos o bancos de datos públicos o privados.

Chile, por su parte, la Ley 19628, 29 de agosto de 1999, sobre protección de la vida privada señala que el tratamiento de los datos de carácter personal se realizará en registros o bancos de datos regidos, tanto por organismos públicos como por particulares.

Guatemala, el artículo 31, Constitución de Guatemala de 1985, reformada en 1993 / Art. 1 numeral 2 Decreto 57-2008, 23/09/2008 y de la Ley de Acceso a la Información Pública, se establece solo el ámbito público porque es solo aplicable a ficheros públicos. Sentado esto, la jurisprudencia limitada a ficheros públicos, aunque por vía jurisprudencial la Corte de Constitucionalidad de Guatemala (2006) incluye ficheros regentados por entes privados, pero desde otros derechos fundamentales como la intimidad personal, la privacidad y el honor.

República Dominicana, en el artículo 44 de la Constitución de República Dominicana de 2010 se establece el derecho de toda persona de acceder a su información y datos sobre ella o sus bienes; hace alusión expresa a que estos consten o reposen en registros oficiales o privados. En el mismo sentido, la Ley 172-13, sale en garantía de los derechos a la intimidad y el honor persona, al respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo, así como al derecho al honor, al buen nombre y a la propia imagen.

d) Se reconoce el ámbito público y de forma limitada o sectorial el ámbito privado

Paraguay, en el artículo 135 de la Constitución se determina que el ámbito de aplicación del *habeas data* son los registros oficiales o privados de carácter público. En suma, se limita a nivel constitucional de protección respecto de ficheros privados. Asimismo, el artículo 8° de Ley 1682 de 2001, que reglamenta la información de carácter privado, señala que los únicos registros protegidos son los oficiales o privados de carácter público o aquellos en manos de entidades que suministren información sobre solvencia económica y situación patrimonial, que pueden ser privados, lo que determinan una protección privada de carácter sectorial.

1.2 Naturaleza del dato

Independientemente de que los países protejan los datos personales desde el derecho a la intimidad, a la privacidad o con el derecho autónomo a la protección de datos personales, mediante garantías constitucionales como el *habeas data* o similares, es condición general definir o explicitar la naturaleza del dato que se protege.

Desde esa perspectiva, se puede concluir ciertos acuerdos básicos:

- *Se usa el término información como sinónimo de dato*

  En Guatemala, Nicaragua, Brasil, Colombia, Paraguay, Perú, Argentina, Venezuela, México, Uruguay, Costa Rica, Chile, Panamá, República Dominicana se utiliza en la normativa vigente el término "información" para definir dato.

  En el caso del Ecuador, existe una posición jurisprudencial de carácter referencial que limita la procedencia del *habeas data* a los datos informativos o con función informativa. Esta postura debe ser aplicada solo en esta garantía jurisdiccional que salvaguarda otros derechos como: el honor, el buen nombre y la intimidad personal y familiar; ya que, en el caso del derecho a la protección de datos personales, el *habeas data* debe adaptarse al contenido de este derecho fundamental y resguardar no solo el dato con contenido informativo, sino también proteger al dato por sí solo, porque aunque inicialmente carece de la característica informativa, puede ser tratado, perfilar a un[1525] individuo y afectar su autodeterminación informativa e incluso otros derechos fundamentales.[1526]

  Por su parte, Bolivia no determina el término información, sino únicamente el de dato registrado; en cambio, Honduras utiliza solamente la terminología dato.

- *Se utiliza el término de dato íntimo*

  Brasil, Argentina, Venezuela, México, Uruguay, Costa Rica, Chile, Panamá, El Salvador y República Dominicana no usa el término dato íntimo en su normativa.

[1525] "Constitución Política de la República de Nicaragua actualizada con las reformas introducidas por la Ley 854 de 2014, de 29 de Enero de 2014 - vLex Global".
[1526] L. NARANJO GODOY, "El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador", *Revista de Derecho Foro*, vol. 27 (2017), 80.

Paraguay contempla el *habeas data* como garantía del derecho a la intimidad. Por eso, protege aquellos datos considerados íntimos debido a que el derecho que se tutela mediante la acción de *habeas data* es el derecho a la intimidad (art. 135 de la Constitución Paraguaya).[1527] En el mismo sentido, Bolivia también protege los datos íntimos, porque consagra el derecho a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación conforme la Constitución boliviana de 2009.[1528]

Perú, en su texto constitucional, numeral 6 del artículo 2,[1529] señala que el *habeas data* protege la información de una persona que afecte su intimidad personal o familiar. Esta visión ha sido superada mediante la Ley 28237 de 2004, Código Procesal Constitucional que desarrolla el proceso de *habeas data* y que supera de forma amplia la cobertura (art. 61). Honduras también determina una postura similar, conforme consta en el artículo 182 de la Constitución de Honduras[1530] que señala que la persona puede promover *habeas data* cuando los datos personales o familiares produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen.

Nicaragua, al describir el recurso de *habeas data*, procede para proteger de la invasión a la privacidad personal y el tratamiento de datos sensibles de las personas en su ámbito íntimo y familiar, así como a favor de toda persona para saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales, es decir autodeterminación informativa. En este sentido Nicaragua protege a través del habeas data, datos sensibles en el ámbito íntimo y familiar (art. 190).[1531]

En el caso del Ecuador, la jurisprudencia señala que el *habeas data* procede para resguardar derechos como el honor, el buen nombre y la intimidad personal y familiar, y también la protección de datos personales. De modo que en Ecuador se protege desde esta acción constitucional también el dato íntimo.

- *Se utiliza el término dato privado*

Colombia utiliza el término dato privado para determinar al dato que, por su naturaleza íntima o reservada, solo es relevante para el titular, conforme la Ley 1266 de 2008.

- *Se utiliza el concepto de dato sensible*

La mayoría de países, independiente de si basan su nivel de protección en la intimidad, la privacidad o la protección de datos personales, establecen esta categoría de datos sensibles, pues se utiliza esta tipología para aplicarles un nivel de protección reforzado. Los países a los que se hace referencia son: Brasil, Guatemala,

[1527] Convención Nacional Constituyente del Paraguay, "Paraguay: Constitución Política de 1992".
[1528] Asamblea Nacional Constituyente de Bolivia, "Constitución Política de 1967, con reformas de 1994, texto concordado de 1995, y reformas de 2002, 2004 y 2005".
[1529] Congreso de la República del Perú, "Perú: Constitución Política de 1993 con reformas hasta 2005".
[1530] Asamblea Nacional Constituyente, "Honduras: Constitución de 1982 modificada por Decreto 381/2005".
[1531] "Constitución Política de la República de Nicaragua actualizada con las reformas introducidas por la Ley 854 de 2014, de 29 de enero de 2014", vLex Global.

Nicaragua, Colombia, Paraguay, Perú, Argentina, Uruguay, República Dominicana, El Salvador, Chile, México, Costa Rica, Panamá y Ecuador.

Por regla general los datos personales sensibles son aquellos relativos a origen racial, étnico, filiación política o pertenencia a sindicatos, a organizaciones sociales, o de derechos humanos (Colombia); convicciones religiosas, filosóficas o morales, relativo a su salud, físicos o psíquicos (Chile y Panamá), presente o futuro (México), vida sexual, los datos biométricos (Perú y Panamá), información biomédica o genética (Costa Rica), antecedentes penales o faltas administrativas, económicos financieros; así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación (Guatemala y Nicaragua). Adicionalmente, ninguna persona puede ser obligada a proporcionar datos sensibles y solo pueden ser recolectados y tratados por razones de interés general en la ley, o con el consentimiento del titular de datos, u ordenados por mandato judicial.

Brasil señala que son datos sensibles aquellos que pertenecen a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este.

Argentina y Uruguay establecen varias condiciones que son necesarias revisar: podrán tratarse datos personales sensibles con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. Se prohíbe la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia católica, las asociaciones religiosas y las organizaciones políticas y sindicales, asociaciones, fundaciones y otras entidades sin fines de lucro, cuya finalidad sea política, religiosa, filosófica, sindical, que hagan referencia al origen racial o étnico, a la salud y a la vida sexual, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio que la comunicación de dichos datos precisará siempre el previo consentimiento del titular del dato.

Por su parte, México señala que los datos sensibles enunciados no son limitativos sino enunciativos, y que por lo tanto cabe calificarse otros que cumplan con los criterios de afectar la esfera íntima, originar discriminación o un posible riesgo grave.

Finalmente, en el caso de Ecuador no existe definición en la normativa constitucional, la cual únicamente al referirse al *habeas data* señala que en el caso de datos sensibles, estos archivos deberán estar autorizados por la ley o por la persona titular y que se exigirá la adopción de las medidas de seguridad necesarias.

Los países que no mencionan la categoría de datos sensibles son: Brasil, Venezuela, Bolivia, Honduras y Panamá.

- *Se utiliza el concepto de dato inocuo*

Esta categoría de dato se aplica a aquellos países que basan su sistema de resguardo de la información de carácter personal en el derecho autónomo e independiente de la protección de datos personales. Esto debido a que para lograr una protección del individuo, se debe proteger cualquier tipo de dato o información personal del

individuo, tal como señala Nicaragua, Perú, Uruguay, Costa Rica o Panamá. Desde esta perspectiva, en ninguno de los países citados aparece de forma expresa el término "inocuo", sino que la redacción para incorporarlo se decanta por la expresión general "todo tipo de dato" o "cualquier información" o como el caso colombiano cualquier pieza de información.

En el mismo sentido, México señala que una persona es identificable cuando pueda determinarse directa o indirectamente mediante cualquier información.

- *Otras categorías de datos*

Varias legislaciones establecen clasificaciones de datos que son aplicables desde las distintas realidades de la región. Así por ejemplo, Brasil establece el dato catastral que es aquel relativo al que la ley autoriza registrar. Asimismo, señala el dato anonimizado que es aquel que no puede ser identificado utilizando medios técnicos razonables y disponibles en el momento de su tratamiento.

Colombia, por su parte, realiza una clasificación particular en virtud de que requiere diferenciar aquellos datos accesibles al público (datos públicos), los que interesan tanto al titular como a terceros interesados (semiprivados), los que solo interesan al titular (privados). En el mismo sentido, Costa Rica clasifica a sus datos en datos personales de acceso irrestricto, contenidos en bases de datos públicas de acceso general, y datos personales de acceso restringido, aquellos que son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.

Paraguay establece una categoría relativa a los datos de solvencia patrimonial o económica. Argentina determina una tipología para establecer distintos niveles de protección, de tal manera distingue los datos sensibles, de los datos informatizados, datos de salud y aquellos relativos a antecedentes penales o contravencionales.

Uruguay señala una lista de tipos de datos para establecer protección en cada caso con la siguiente enumeración: dato sensible, datos personales relativos a la comisión de infracciones penales, civiles o administrativas, datos relativos a salud, datos de telecomunicaciones, o bases de datos con fines de publicidad.

Chile clasifica sus datos en dato estadístico y dato crediticio, con lo que alude a la finalidad para establecer su particular regulación.

Perú establece categorías de datos asociados a los bancos que los contienen, de tal forma que menciona bancos de datos personales, bancos de datos personales de administración privada, bancos de datos personales de administración pública y fuentes accesibles.

República Dominicana determina datos personales, datos de salud, datos informáticos, información crediticia e información pública.

Panamá, conceptualiza datos confidenciales, como aquellos que no deben ser de conocimiento público; datos anónimos, que son aquellos cuya identidad no puede ser establecida por medios razonables; y, dato disociado, que es aquel que no puede asociarse al titular.

Finalmente, Ecuador establece una categoría que es la de carácter informativo del dato incluido en una jurisprudencia y que solo es aplicable al *habeas data* que protege otros derechos fundamentales distintos a la protección de datos personales, esto es el honor, buen nombre, imagen y voz de la persona y la intimidad.

- *Se usan otros términos como: documentos, datos genéticos, bancos o archivos de carácter personal, entre otros*

Es común el uso de terminología asociada con la representación, manifestación del dato o la información personal que, lejos de ayudar a clarificar, dificulta la comprensión y el ámbito de aplicación del derecho.

En este sentido, la legislación mayoritaria prefiere utilizar términos como archivo, *registro* (Panamá), ficheros, *fichas* (Guatemala) base o banco de datos *u otros medios técnicos* (Nicaragua), indistintamente, comprendiendo a cualquiera de ellos como el conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad o forma de su formación, almacenamiento, organización o acceso (República Dominicana, Colombia, Uruguay, Brasil y Panamá), cualquiera que sea la modalidad de uso, elaboración, organización o acceso (Costa Rica y Argentina), formación, almacenamiento (Uruguay).

Sin embargo, los siguientes países utilizan nomenclatura que, lejos de ayudar a homogeneizar el sistema de resguardo, dificulta su comprensión y aplicación. Este es el caso de Paraguay, que establece al registro como un repositorio documental ordenado a los efectos de su compulsa; es decir, no hace alusión a bases de datos, archivos o términos similares que permitan interpretar que su soporte sea informático. Venezuela, por su parte, utiliza los términos registros oficiales o privados y no bases o bancos de datos, que no es concluyente para determinar si se trata o no de procesos informáticos o automatizados. Utiliza también el término "documento", determinando que este podrá ser de cualquier naturaleza con tal que contenga información cuyo conocimiento sea de interés para comunidades o grupos de personas.

Finalmente, Ecuador evidencia una dificultad en el artículo 92 de la Constitución de 2008, que regula la garantía constitucional de *habeas data*, ya que no existe mención expresa a los términos genéricos "datos" e "información". Por el contrario, la garantía constitucional se encontraría incompleta y sería insuficiente para determinar un adecuado marco de protección porque se debe proteger al dato y a la información, y no solo a sus manifestaciones o procesamientos, precisamente para evitar que en el avance de la tecnología existan datos que pudieran quedar fuera del régimen de protección por no calzar alguna de las expresiones constantes en la norma, esto es *documentos, datos genéticos, bancos o archivos de datos personales e informes sobre sí misma, o sobre sus bienes*. Tanto la norma que hace alusión al derecho fundamental, como aquella que consagra la garantía constitucional del *habeas data* deben proteger el acceso, decisión y gestión del dato o de la información, incluidos de forma expresa los datos genéticos, en cualquier soporte físico virtual, ya sean que estos consten en documentos o informes, se encuentren de forma aislada o incorporados a archivos o bancos de datos, sean parte o no de

cualquiera otra forma de recogida o procesamiento y versen sobre la persona misma o sobre sus bienes. La única condición clara y coincidente es que estos datos deben vincularse a personas identificadas o identificables, no necesariamente íntimos, sino que todo tipo de dato personal incluso aquel considerado inocuo que amerita protección en virtud de su potencialidad y de los actuales avances en minería de datos y la elaboración de perfiles.[1532]

- *Dato asociado a la persona identificada o identificable*

Aun si el sistema de salvaguarda de los datos se asocia a la intimidad, la privacidad o a la protección de datos personales, coincide como elemento esencial la condición de que el dato debe estar asociado o vinculado a la persona para que amerite protección.

En líneas generales, la mayoría de normativa establece que se protege el dato personal, es decir, cualquier información concerniente (Guatemala, México, Bolivia, Chile, Panamá y República Dominicana), vinculadas, asociadas (Colombia), relacionada (Brasil), o sobre (Nicaragua), o referida a (Argentina, Uruguay), o relativo (Costa Rica) a personas naturales identificadas o identificables (Guatemala, Brasil, México, Bolivia, Costa Rica, Chile, Panamá y República Dominicana), o que la identifica o la hace identificable (Nicaragua, Perú), o determinadas o determinables (Uruguay, Argentina).

Perú realiza una precisión adicional: establece que la identificación debe realizarse a través de medios que pueden ser razonablemente utilizados. México, además, determina que debe considerarse que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente mediante cualquier información.

Existe un grupo de países, entre los que se incluye Ecuador, que al describir las acciones constitucionales de *habeas data*, a más de señalar que se trata de datos personales, hacen alusión a que estos son datos sobre sí mismos o de sus bienes (Paraguay, Venezuela).

El caso de Honduras que al describir el dato señala que estos son personales o familiares, de tal forma que se determina una condición que se asocia a sistemas de protección asociados con la intimidad y que no permiten proteger a la persona ni garantizarle sus derechos de autodeterminación informativa.

Finalmente, otro grupo de países no consagra definición alguna, sino que hace alusión a que son datos de carácter personal como es el caso de Panamá.

- *Tipo de soporte que contiene el dato personal*

Es necesario recalcar que se protege el dato personal independientemente del soporte que lo contenga, sea este físico o virtual, automatización o manual, soporte *físico como el electrónico* (Brasil, Nicaragua, Colombia, Panamá y México) o con la afirmación general estén en *formato electrónico o no* (Argentina y República

[1532] NARANJO GODOY, "El dato personal".

Dominicana), puesto que lo sustancial es que se encuentre registrado o almacenado junto a otros datos (Brasil).

Por su parte, México señala que los datos personales podrán constar tanto en documentos como en expedientes; es decir, se protege cualquier modo de organización de la información, en todas las formas posibles de soporte, incluidos los escrito, impreso, sonoro, visual, electrónico, informático u holográfico, *medio físico o magnético* (Bolivia), convencionales (Honduras), *digital, óptico* (Perú), químico, físico o biológico (Panamá).

Y en cuanto al soporte electrónico del uso de la frase "otros medios técnicos", se colige que la lista es meramente ejemplificativa, lo que al menos no limita en este aspecto la procedencia del *habeas data* (Nicaragua). De esta forma, se establece una lista ejemplificativa de cuales son la variedad de formatos en los que puede constar un dato personal que no necesariamente son informáticos, sino que pueden ser escritos y materializados en otro tipo de tecnologías.

Estas posiciones de corte integral en la salvaguarda del derecho, se contraponen con la visión venezolana que establece que se protege los registros oficiales o privados y no bases o bancos de datos, con lo que no se asocia el término únicamente a procesos informáticos o automatizados, sino que pareciera referirse a registros de datos físicos.

De otro lado, otros países no hacen mención al tipo de soporte, pero por la generalización se entiende incluido tanto el físico como el virtual, como es el caso de Guatemala, Paraguay y El Salvador, o como el caso del Uruguay en el cual expresamente se menciona bajo cualquier soporte *o medio* (Panamá).

De lo señalado, debido a lo mutable de las tecnologías es preferible un régimen abierto en el cual se obvie señalar el tipo de soportes para evitar dejar por fuera alguno, en el caso de optar por una lista. Es indispensable aclarar que esta es meramente ejemplificativa porque se protege el dato personal indistintamente del medio que lo contenga.

1.3 Sujeto activo

Para la realización del análisis de sujetos activo es necesario que desde la normativa constitucional o legal de los diversos países latinoamericanos, se identifique el derecho o los derechos que salvaguardan los datos personales: intimidad, privacidad o protección de datos personales. Con la finalidad de que, una vez referido el derecho, se pueda determinar el titular del mismo; es decir, el sujeto activo.

Respecto de aquellas realidades en las que existe garantía o acción constitucional, la legitimación activa se analizará cuando se revise *habeas data*, amparo, acción de privacidad o tutela conforme se regule en cada legislación. El país en el cual no existe derecho de protección de datos personales, sino únicamente *habeas data*, es Paraguay.

Respecto de la determinación del sujeto activo o titular de un derecho, se debe distinguir los supuestos siguientes:

a) Titulares activos del derecho a la intimidad y a la privacidad

El Salvador (ámbito público exclusivamente) y Venezuela protegen los datos personales desde el enfoque de la intimidad; se utiliza la expresión "toda persona". Bolivia utiliza el enunciado "las bolivianas y los bolivianos". Chile, Honduras y Paraguay, por su parte, no utilizan una frase específica, sino que la norma hace referencia a las personas en general.

Ahora bien, cuando se usa la locución "toda persona" se discute si los titulares son tanto las personas naturales como los jurídicos públicos y privados, o si es necesario que el Estado deje expresa constancia de que una persona jurídica puede ser titular de estos derechos. Desde esta perspectiva, se colige lo siguiente:

Tabla 1

País	Persona natural	Persona jurídica pública	Persona jurídica privada	Otro titular
Bolivia	SI.	NO.	NO.	NO.
Chile	SI.	NO.	NO.	NO.
El Salvador	SI.	SI.	SI.	NO.
Guatemala	SI.	NO.	NO.	NO.
Honduras	SI.	NO.	NO.	NO.
Paraguay	SI.	NO.	SI (reconoce la Corte Suprema del Paraguay).	NO.
República Dominicana	SI.	NO.	NO.	NO son titulares las personas fallecidas.
Venezuela	SI.	NO.	NO.	Comunidades o grupos de personas y Defensor del Pueblo.

Fuente y elaboración: La autora (2018).

De lo señalado en la tabla 1, se concluye que por regla general no se acepta como titular del derecho a la intimidad a las personas jurídicas, sean estas públicas o privadas, porque la forma de protección de los datos está atada al derecho a la intimidad, que por su naturaleza propia es solo titular la persona natural.

b) Titulares activos del habeas data (como derecho) o del derecho a la protección de datos personales

Señalan la frase generalizada "toda persona" los países Argentina, Perú, Colombia, Nicaragua, República Dominicana, y Guatemala (este último, desde su visión limitada de carácter sectorial atinente únicamente a lo público). Por su parte, Brasil y Panamá usa la frase "persona natural". Ecuador, Uruguay y Costa Rica no utilizan la locución citada, pero se refieren a las personas en general. Finalmente, México utiliza el enunciado general "toda persona" y precisa que el titular no requiere la necesidad de que se acredite interés alguno o se justifique su utilización.

Tabla 2

País	Persona natural	Persona jurídica pública	Persona jurídica privada	Otro titular
Argentina	SI.	NO.	SI (aquellas con domicilio legal o delegaciones o sucursales en el país).	Datos de personas fallecidas, corresponderá a los sucesores universales la titularidad del derecho de acceso.
Brasil	SI	NO	NO	Datos personales niños y adolescentes como titulares de derechos, solo podrán tratarse en su mejor interés, con el consentimiento específico y destacado dado por al menos uno de los padres o el responsable legal, en su artículo 14 LPDP
Colombia	SI.	SI (solo para solicitud de información en ejercicio de sus funciones legales o por orden judicial).	SI (la protección se extienda a las personas jurídicas cuando se afecten los derechos de las personas que la conforman).	Terceros autorizados por el titular del dato.
Costa Rica	SI.	NO.	NO.	NO.
Ecuador	SI.	NO.	SI (se analizará cada caso particular respecto de persona jurídica, comunidad, pueblo, nacionalidad y colectivo).	Comunidades, pueblos, nacionalidades y colectivos; procede de datos propios y distintos de los miembros.
México	SI.	NO.	NO.	NO.
Nicaragua	SI.	NO.	SI.	Datos de personas fallecidas; corresponderá a los sucesores universales, que deberán probar su condición de herederos.
Panamá	SI.	NO.	NO.	NO.
Perú	SI.	NO.	SI (reconocimiento jurisprudencia, mediante el expediente 4739-2007-PHD.	NO.
Uruguay	SI.	NO.	SI (por extensión a las personas jurídicas en cuanto le corresponda).	Datos de personas fallecidas; corresponderá a los sucesores universales, que deberán probar su condición de herederos.

Fuente y elaboración: La autora (2018).

De lo señalado en tabla 2, se concluye que por regla general no se acepta como titular del derecho a la protección de datos personales a las personas jurídicas, sean estas públicas o privadas.

Entre tanto, Panamá en su Ley 81 y Brasil en su LPDP que para efectos de esta Ley, se considera titular de los datos únicamente a la persona natural a la que se refieren los datos, dejando de lado a personas morales. Colombia es el único país que limita esa titularidad exclusivamente para la solicitud de información en ejercicio de sus funciones legales o por orden judicial. Mientras que los siguientes países reconocen como titulares a personas jurídicas privadas: Uruguay, Perú, Panamá, Ecuador, Colombia, Nicaragua y Argentina, siendo necesario en la mayoría de ellos analizar cada caso.

Finalmente, respecto de otros titulares, se distinguen los datos de personas fallecidas, cuyos titulares serán sus herederos universales. Y el caso especial del Ecuador, que reconoce como titulares a comunidades, pueblos, nacionalidades y colectivos procede de datos propios y distintos de los miembros.

1.4 Sujeto pasivo

Tal como se realizó previamente, para el análisis de los sujetos pasivos es necesario que desde la normativa constitucional o legal de los diversos países latinoamericanos, se identifique el derecho o los derechos que salvaguardan los datos personales: intimidad, privacidad o protección de datos personales.

Respecto de aquellas realidades en las que existe garantía o acción constitucional, la legitimación pasiva se analizará cuando se revise las acciones de *habeas data*, amparo, acción de privacidad o tutela, conforme se regule en cada legislación. Paraguay reconoce exclusivamente al *habeas data*.

Desde una aproximación general se distinguen varios sujetos pasivos, acorde con su nivel de participación en el tratamiento de la base de datos puesta en su conocimiento y procesamiento: responsable, encargado, tercero, destinario y otros casos especiales.

Como se efectuó anteriormente, para la determinación del sujeto pasivo u obligado a respetar y cumplir con el contenido del derecho, se debe distinguir varios supuestos:

a) Sujetos pasivos del derecho a la intimidad y a la privacidad

En la tabla 3 se concluye que se considera como responsable al sujeto pasivo u obligado del derecho a la intimidad ya sean estas personas naturales o jurídicas, públicas o privadas. No existen otras definiciones aplicables a sujetos pasivos puesto que las figuras del encargado, tercero, destinatarios, usuarios y otros son propios de derecho a la protección de datos personales.

Tabla 3

País	Responsable	Encargado	Tercero	Destinatario	Otro
Bolivia	Quien está a cargo de los archivos o bancos de datos, sean estos públicos o privados.	NO.	NO.	NO.	NO.
Chile	Persona natural o jurídica privada, o el respectivo organismo público, a quienes competen las decisiones relacionadas con el tratamiento de los datos de carácter personal.	NO.	NO.	NO.	NO.
El Salvador	Entidades públicas como entes obligados a garantizar la exactitud de los datos personales (ámbito público exclusivamente).	NO.	NO.	NO.	NO.
Honduras	NO	NO.	NO.	NO.	NO.
Paraguay	Responsables de los registros oficiales o privados de carácter público que contienen datos personales.	NO.	NO.	NO.	NO.
Venezuela	Aquellos que tienen a su cargo los registros oficiales o privados.	NO.	NO.	NO.	NO.

Fuente y elaboración: La autora (2018).

b) Sujetos pasivos del habeas data (como derecho) o del derecho a la protección de datos personales

La mayoría de los países que protegen este derecho, desde la perspectiva de la protección de datos personales, reconocen las figuras del responsable y el encargado, excepto Argentina que no recoge la figura del encargado. El "tercero" es un obligado reconocido por Argentina, México, República Dominicana y Uruguay. Por su parte, solo Uruguay y República Dominicana incluyen en este reconocimiento a la figura del destinatario, anotándose que este último reconoce este derecho desde la perspectiva de la intimidad, privacidad, honor e imagen. Argentina, República Dominicana y Uruguay, además, introducen al usuario de datos. Otros países como México, Colombia recogen además otros obligados de forma ejemplificativa, de tal forma que no se quede fuera ningún sujeto pasivo.

Tabla 4

País	Responsable	Encargado	Tercero	Destinatario	Otro
Argentina	Responsable de archivo, registro, base o banco de datos será la persona física o de existencia ideal, pública o privada, que es titular de un archivo, registro, base o banco de datos. / Responsables de ficheros de información crediticia.	NO.	El tratamiento puede darse por cuenta de terceros, quienes no podrán aplicar o utilizar los datos con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.	NO.	Usuario de datos se considera a toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.
Brasil	Se menciona la palabra Controlador: Persona natural o jurídica, de derecho público o privado, a quien competen las decisiones referentes al tratamiento de datos personales.	Se menciona el término operador que es la persona natural o jurídica, de derecho público o privado, que realiza el tratamiento de datos personales en nombre del controlador.	NO.	NO.	Se usa el término responsable para la persona natural, indicada por el controlador, que actúa como canal de comunicación entre el controlador y los titulares y la Autoridad Nacional de Protección de Datos (delegado de protección)
Colombia	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros decida sobre la base de datos y/o el tratamiento.	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros realice el tratamiento de datos personales por cuenta del responsable del Tratamiento.	NO.	NO.	Fuente de información. Operador de la información. Usuario. Agencia de Información. Comercial.
Costa Rica	Persona física o jurídica de entidad pública o privada que administre, gerencia o se encargue de la base de datos y con arreglo a la ley determine su finalidad, registrando el procedimiento a aplicar.	El encargado da tratamiento a los datos personales por cuenta del responsable de datos.	NO.	NO.	Intermediario tecnológico o proveedor de servicios: brinda servicios de infraestructura, plataforma, *software* u otros.
Ecuador	Toda persona que recolecte, archive, procese, distribuya o difunda datos o información (*habeas data*).	NO.	NO.	NO.	NO
Guatemala	Solamente el Estado es el administrador y responsable del fichero.	NO.	NO.	NO.	NO
México	Persona física o jurídica, pública o privada de carácter privado que decide sobre el tratamiento de datos personales.	Persona física o jurídica, público o privada, que sola o conjuntamente con otras trate datos personales por cuenta del responsable.	Persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.	NO.	Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos

					públicos. Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables.
Nicaragua	Toda persona natural o jurídica, pública o privada, que decide sobre la finalidad y contenido del tratamiento de los datos personales.	NO.	NO.	NO.	NO
Panamá	Art.17, de la Ley 81 señala que "Responsable del tratamiento de los datos. Persona natural o jurídica, de derecho público o privado, lucrativa o no, que le corresponde las decisiones relacionadas con el tratamiento de los datos y que determina los fines, medios y alcance, así como cuestiones relacionadas a estos."	Custodio dela base de datos es la "persona natural o jurídica, de derecho público o privado, lucrativa o no, que actúa a nombre y por cuenta del responsable del tratamiento y le compete la custodia y conservación dela base de datos.	NO.	NO.	NO
Perú	Son titulares de los bancos de datos personales cuando determinan la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.	Aquellos que sola o actuando conjuntamente con otros realizan el tratamiento de los datos personales por encargo del titular del banco de datos personales.	NO.	NO.	NO
República Dominicana (reconoce el derecho desde la intimidad, privacidad, honor e imagen)	Persona, pública o privada, titular del archivo de datos personales que decide la finalidad, el contenido, los medios del tratamiento y el uso de la información obtenida con el tratamiento de los datos personales.	Persona física o jurídica, pública o privada, que realice el tratamiento de los datos personales por cuenta del responsable del tratamiento.	Persona física o jurídica, pública o privada, u órgano administrativo distinto del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.	Persona física o jurídica, pública o privada, u órgano administrativo, al que se revelen los datos.	Usuario de datos, suscriptor o afiliado es toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos. Igualmente, las entidades de intermediación financiera, los agentes económicos, las entidades públicas, y las demás personas físicas o jurídicas que mantengan acuerdos con las Sociedades de Información Crediticia (SIC) para acceder a las informaciones de los consumidores.
Uruguay	Persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.	Persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento.	Persona física o jurídica, pública o privada, distinta del titular del dato, del responsable de la base de datos o tratamiento, del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento.	Persona física o jurídica, pública o privada, que recibiere comunicación de datos, se trate o no de un tercero.	Usuario de datos es toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos.

Fuente y elaboración: La autora (2018).

1.5 Objeto o bien jurídico

1.5.1 Derecho de información

a) Respecto del derecho a la intimidad y a la privacidad

Paraguay, se refiere expresamente al derecho de información para conocer su uso y finalidad de datos íntimos y sensibles.

El Salvador, cuya normativa solo se refiere al ámbito público, señala el derecho de información respecto del procesamiento de los datos personales y por qué y a quién fueron transmitidos.

Mientras, *Venezuela* determina el derecho a conocer el uso que se haga de sus datos personales y la finalidad de la recogida de estos.

Bolivia, por su parte, protege a toda persona que haya sido indebida ilegalmente impedida de conocer datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados.

Guatemala reconoce el derecho de información respecto del registro y finalidad de los datos, pero solo en ficheros manejados por el Estado.

El caso de *República Dominicana* es especial, puesto que reconoce el derecho de información con todos sus elementos básicos (finalidad, existencia e identidad del responsable e incluso sobre acciones pertinentes), pero como a nivel constitucional y legal consta que no reconocen el derecho a la protección de datos personales, sino que garantizan de los derechos a la intimidad y el honor personal, al respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo, así como al derecho al honor, al buen nombre y a la propia imagen. Este sistema de protección resulta aún ineficiente.

Chile y Honduras no desarrollan el contenido de este derecho.

Pese a que dos países no recogen este derecho, de lo analizado se puede colegir que el deber de información resulta necesario para la protección de los datos personales (Venezuela), ya sea que su enfoque esté limitado a datos íntimos o sensibles (Paraguay), procedente solamente en caso de negativa de conocer (Bolivia), desde la perspectiva de lo público (El Salvador).

b) Respecto del derecho a la protección de datos personales

Tabla 5

País	Derecho de Información	Finalidad	Existencia	Identidad de los responsables	Otro
Argentina	Toda persona puede solicitar información al organismo de control relativo a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita.	SI.	SI.	SI.	Derecho de información junto con el de consulta pública y gratuita.
Brasil	El derecho de información se encuentra evidenciado en el principio de transparencia recogido en el artículo 6, 9 y 18 de la LGPD por el cual "el titular tiene derecho a un fácil acceso a la información sobre el procesamiento de sus datos, que debe estar disponible de manera clara, apropiada y abierta" (artículo 9 de la LGPD),	SI	SI	SI (obliga a informar sobre las entidades públicas y privadas con las cuales el controlador realizó uso compartido de los datos	no
Colombia	Derecho a conocer informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades	SI.	SI.	De entidades públicas y	Carácter facultativo de la respuesta;

	públicas y privadas. El artículo 12 de la Ley 1266 de 2008 señala el derecho de informar sobre el tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; el carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes; Los derechos que le asisten como Titular; La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento. La obligación del responsable del tratamiento de conservar prueba del cumplimiento.			privadas. La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.	derechos que le asisten como Titular; de conservar prueba del cumplimiento.
Costa Rica	Consta este derecho como consecuencia del deber de información constante en el artículo 5 referido al consentimiento informado.	NO.	NO.	NO.	No consta expresamente.
Ecuador	Derecho a conocer de la existencia, finalidad, origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.	SI.	SI.	SI (origen y destino).	Tiempo de vigencia.
México	El derecho de información se materializa a través del aviso de privacidad al que está sujeto el tratamiento. La finalidad, la existencia y los sujetos obligados.	SI.	SI.	SI.	Aviso de privacidad Acceso.
Nicaragua	Toda persona tiene derecho a conocer de toda información que sobre ella se haya registrado en las entidades de naturaleza privada y pública, así como el derecho de saber por qué y con qué finalidad se tiene esa información.	SI.	SI.	Entidades de naturaleza privada y pública.	NO.
Panamá	NO Sólo se reconoce como principio de transparencia (artículo 2 de la Ley 81).	NO.	NO.	NO.	NO.
Perú	"ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del encargado del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello. Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables" (art. 18, LPDP).	SI.	SI.	SI.	Identidad, el carácter obligatorio o facultativo de sus respuestas; la transferencia de los datos personales; las consecuencias; el tiempo; la posibilidad de ejercer los derechos que la ley le concede; si son recogidos en línea a través de políticas de privacidad.
Uruguay	Informar previamente a sus titulares en forma expresa, precisa e inequívoca: la finalidad y destinatarios de los datos tratados, la existencia de la base de datos.	SI.	SI.	SI.	NO.

Fuente y elaboración: La autora (2018).

De los países que reconocen a nivel constitucional o legal el derecho a la protección de datos personales únicamente Panamá y Costa Rica no reconocen el derecho de información; sin embargo, en el caso de este último consta como condición para la eficacia del consentimiento informado, pero no ha sido desarrollado como derecho independiente.

Los ocho países restantes coinciden en consagrar el derecho de información como parte integrante del contenido esencial del derecho a la protección de datos personales, señalando además como elementos sustanciales los relativos al conocimiento sobre la finalidad, la existencia y la identidad de los responsables. En el caso del Ecuador, estos

elementos constan descritos en el *habeas data*; entonces, es necesario que la normativa desarrolle una ley específica que lo regule como parte del derecho en sí mismo.

Las normas más completas son la brasileña, la peruana, la colombiana y la mexicana (entre las varias leyes que regulan la materia) que incluyen como elementos básicos del derecho de información: el de conocer los datos o la existencia de la base de datos o registro, la finalidad del procesamiento, uso o tratamiento, así como la identidad de los destinatarios, responsables, encargados, sean estos personas públicas o privadas. Además, el carácter facultativo de las respuestas sobre todo en caso de datos sensibles o sobre niños, niñas o adolescentes; los derechos que le asisten como titular; la obligación de conservar prueba del cumplimiento; el tiempo de vigencia y el aviso de privacidad, tanto si son recogidos en línea o no.

1.5.2 Autodeterminación informativa

a) Respecto del derecho a la intimidad y a la privacidad

Bolivia no reconoce la autodeterminación informativa, ya que el artículo 130 determina expresamente que la acción de protección de privacidad protege de aquella afectación a los derechos fundamentales a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, y que no procederá para levantar el secreto en materia de prensa.

Guatemala no reconoce este derecho porque se refiere a ficheros públicos exclusivamente.

En el mismo caso se encuentra *El Salvador*; aunque su reconocimiento, como se vio en líneas anteriores, se realiza mediante precedentes jurisprudenciales dictados por la Corte Suprema de Justicia de El Salvador conforme resoluciones de amparo 118-2002, acción de inconstitucionalidad 36-2004 y de amparo 934-2007; sin embargo, lamentablemente su ámbito de aplicación a nivel normativo se limita al ámbito público.

República Dominicana, tanto en el artículo 44 de la Constitución como en el artículo 1 de la Ley 172-13, señalan que la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, provienen en garantía de los derechos a la intimidad y el honor personal, al respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo, así como al derecho al honor, al buen nombre y a la propia imagen.

En *Chile*, *Honduras*, *Paraguay* y *Venezuela* no existe ni reconocimiento constitucional, ni legal ni jurisprudencial sobre el derecho a la autodeterminación informativa como elemento sustancial.

Es obvio que, desde la limitada perspectiva de los derechos a la intimidad o privacidad como salvaguarda de los datos personales, no se reconoce a la autodeterminación informativa. Por eso, los países estudiados no la incluyen ni remotamente.

b) Respecto del habeas data (como derecho) o del derecho a la protección de datos personales

Argentina, el artículo 43 de la Constitución argentina de 1994 reconoce al *habeas data* como subtipo de amparo que tiene por finalidad tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. De esta manera, se reconoce una de las facetas de la autodeterminación informativa; sin embargo, este derecho no es absoluto sino limitado a la necesidad de probar que los datos son falsos, o por medio de ellos se produce discriminación en su contra. Respecto al derecho de revocación, solo consta expresamente establecido para el caso de las cesiones (núm. 2, art. 11, LPDP).

Brasil, señala en los artículos 1 y 2 del LGPD establecen la protección a los derechos fundamentales de libertad; privacidad; autodeterminación informativa; libertad de expresión, información, comunicación y opinión; inviolabilidad de la intimidad, honor e imagen; el desarrollo e innovación económica y tecnológica; la libre empresa, libre competencia y protección del consumidor; y los derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por parte de personas naturales. Asimismo, el artículo 17 del LGPD hace alusión a la titularidad de la persona sobre su dato, como atribución de sus poderes de decisión o control que son el reconocimiento de la autodeterminación informativa como garantía de los otros derechos citados.

Colombia, la autodeterminación informativa como contenido inherente del derecho a la protección de datos es producto de la interpretación de la jurisprudencia constitucional colombiana que incluye en el *habeas data* a la autodeterminación informativa y a la libertad informática.[1533]

Costa Rica, en los considerandos de la Ley 8968, determina que esta norma de orden público tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. Esta aproximación es la más completa respecto del alcance, dimensión autónoma e instrumental de la protección de datos personales como derecho.

Ecuador consagra en el artículo relativo a las libertades fundamentales, el derecho a la protección de datos personales, y determina la dimensión relativa a la autodeterminación informativa cuando menciona expresamente como derecho absoluto del titular el de decidir sobre su información y datos personales.

México, si bien la Constitución mexicana determina en el artículo 16 el derecho de toda persona al acceso, rectificación y cancelación, también incluye el derecho a oponerse, esto es que, excepto en los casos expresamente autorizados por la ley, el titular puede negarse a que sus datos sean recopilados. De modo que una de las manifestaciones directas del derecho a la autodeterminación informativa consta reconocida en la

[1533] Corte Constitucional de Colombia, "Sentencia C-748/11".

Constitución citada. En el mismo sentido, el artículo 1 de la LFPDPPP de 2010 señala que esta tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas (art. 1).

Nicaragua, si bien la Constitución nicaragüense de 1995 no reconoce la autodeterminación informativa de forma expresa, así como tampoco utiliza las expresiones "decidir" u "oponerse"; sin embargo, el considerando quinto de la Ley de Reforma y Adiciones a la Ley 49, "Ley De Amparo", Ley 831 aprobada el 30 de enero del 2013, incluye por primera vez la garantía legal de habeas data que "sirve como mecanismo jurisdiccional de protección de los derechos a la autodeterminación informativa y complementa los mecanismos de control de la Constitución que establece la cita Ley".

Asimismo, el artículo 1 de la Ley de Protección de Datos Personales de 2012 señala que su objeto es el resguardo de la información personal como garantía de los derechos fundamentales a la privacidad personal y familiar y al derecho a la autodeterminación informativa. Ahora bien, el artículo 3, que define varios términos de la citada ley, al describir qué es la autodeterminación informativa dice que "Es el derecho que tiene toda persona a saber quién, cuándo, con qué fines y en qué circunstancias toman contacto con sus datos personales".[1534]

Lamentablemente, esta definición además de incompleta causa confusión, puesto que la autodeterminación no se limita al acceso como una de las facultades subjetivas de los titulares, sino que se refiere a la posibilidad de decidir de forma general sobre cualquier aspecto relativo a sus datos personales, incluso a oponerse a su recolección.

En *Panamá* es a través de la Ley 81 sobre la protección de datos personales que se reconoce la autodeterminación informativa, pues el titular tiene derechos de acceso, rectificación, cancelación y oposición.

Perú, si bien el numeral 6 del artículo 2 de la Constitución de la República del Perú de 1993 protege la información de una persona que afecte su intimidad personal o familiar, el Tribunal Constitucional del Perú, en expediente 1797-2002-HD/TC, 29 de enero de 2003, amplió el rango de cobertura y reconoció a la autodeterminación informativa con un contenido distinto del derecho a la intimidad, la imagen e incluso de la identidad. Por eso, el artículo 61 de la Ley 28237 de 2004, Código Procesal Constitucional, determinó la facultad del titular de acceder, conocer, actualizar, suprimir, incluir o rectificar sus datos personales sin la necesidad de que esta información afecte o haya afectado la intimidad personal o familiar.

Uruguay, en su Carta Magna no reconoce de forma expresa a la autodeterminación informativa, pero se considera reconocida al estipular el artículo 72 de la Constitución de la República que la norma constitucional no excluirá otros derechos inherentes a la personalidad humana. Aún más, con la aprobación de la Ley 18.331, de Protección de Datos Personales y Acción de Habeas Data, 11 de agosto de 2008, que desarrolla todo el marco de regulación del derecho a la protección de datos personales como un derecho

[1534] "Ley No. 787, Ley de Protección de Datos Personales de Nicaragua, de 29 de marzo de 2012", - vLex Global.

humano inherente a la dignidad de persona, reconoce al derecho como autónomo e independiente y por ende a su contenido caracterizante, esto es la autodeterminación informativa.

Se puede concluir, entonces, que la mayoría de países que reconocen el derecho a la protección de datos personales lo hacen desde el reconocimiento a la autodeterminación informativa como parte de su contenido esencial e inherente. Aunque, no existe unanimidad sobre su alcance, tal es así que en varios casos no se desarrolla su definición o se lo contextualiza equivocadamente con la privacidad. Finalmente, se puede concluir también que es elemento básico común de la autodeterminación informativa la libertad del titular de decidir u oponerse a cualquiera de los derechos o principios propios de este sistema de protección, aunque hay alguna legislación (Argentina) que aún sujeta esta libertad a la naturaleza errónea o discriminatoria del dato o su tratamiento y no a la simple voluntad del titular.

1.5.3 Necesidad de mandato legal para tratamiento sin autorización del titular

a) Respecto del derecho a la intimidad y a la privacidad

Bajo el enfoque de derechos a la intimidad y a la privacidad, se requiere mandato de ley para acceder, recopilar, proporcionar o divulgar datos personales para acciones, aspectos específicos, en los países registrados en la tabla 6 que consta a continuación:

Tabla 6

País / Norma	**Mandato legal**	**Acceder**	**Recopilar**	**Proporcionar entre entes públicos**	**Divulgar entre entes públicos**	**Relativos a niños, niñas y adolescentes**	**Finalidades no prohibidas**	**Datos sensibles**
El Salvador, Art. 34, Ley 534-2011.	SI.	NO.	NO.	SI.	SI.	NO.	NO.	NO.
Venezuela, Art. 28, Constitución.	SI.	SI.	NO.	NO.	NO.	SI. Art. 78, Ley de Infogobierno. Solo previa solicitud de la persona legitimada, el Poder Público y el Poder Popular pueden recopilar y utilizar datos de niños, niñas y adolescentes para las finalidades siempre relacionadas a sus derechos y garantías.	NO.	NO.
Chile, Art. 4, Ley 19628.	SI.	NO.	NO.	NO.	NO.	NO.	NO.	SI. Art. 10, Ley 19628.
Guatemala, Ley de Acceso a la Información	SI. Art. 32.	NO.	NO	SI. Art. 32.	NO.	NO.	NO.	SI, art. 32, en ningún caso se podrán crear bancos de datos o archivos con

Pública.								datos sensibles o datos personales sensibles, salvo para el servicio y atención propia de la institución.

Fuente y elaboración: La autora (2018).

Asimismo, desde el enfoque de la intimidad y privacidad, la recopilación, uso, tratamiento y cesión de datos personales se faculta por ley, aun sin autorización del titular, para casos o contextos específicos expresamente señalados, como los que constan a continuación:

Tabla 7

País / Norma	**Estadísticas, científicas**	**Interés general**	**Ejercicio de competencias públicas**	**Investigación de delitos**	**Investigación de infracciones administrativas**	**Orden judicial**	**Contenidos en registros públicos**	**Contratación de servicios de terceros para tratamiento de datos**
El Salvador, Art. 34, Ley 534-2011.	SI.	SI.	SI.	SI.	SI.	SI.	NO.	SI. Los terceros no podrán utilizar con propósitos distintos para los cuales se proporcionaron y serán responsables de su actuación.
Venezuela, Art. 28, Constitución.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Chile; Art. 4, Ley 19628.	NO.	NO.	SI. Art. 20. "Sólo podrá efectuarse respecto de las materias de competencia del ente público".	SI. Art. 21. "Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena".	NO.	SI. Art. 21. "Exceptuase los casos que sea solicitada por los tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia".	NO	NO.
Guatemala, Ley de Acceso a la Información Pública	SI. Art. 32.	SI. Art. 32.	SI. Art. 32.	NO.	NO.	SI. Art. 32.	SI. Art. 32.	NO.

Fuente y elaboración: La autora (2018).

Adicionalmente, existen prohibiciones absolutas; es decir, ciertos casos que existe prohibición expresa que impide recopilar datos, usarlos, tratarlos o cederlos estos son:

Tabla 8

País / Norma	Fuentes periodísticas	Profesiones establecidas por ley
Venezuela,	Prohibido.	Prohibido.
Art. 28 de la Constitución.		

Fuente y elaboración: La autora (2018).

El caso especial del *Paraguay* establece que los ficheros materia de regulación son los considerados *registros oficiales o privados de carácter público* (Ley 1682-2001); es decir, los datos contenidos en ellos están autorizados y regulados por la ley, por lo que el mandato legal es la regla general y la excepción, el consentimiento.

Finalmente, existen países que no hacen referencia alguna a la necesidad de mandato legal para tratamiento de datos personales sin autorización del titular, así como tampoco se detallan casos expresos en los que se ha ponderado o justificado por el legislador la necesidad de autorización legal. Estos países son *Bolivia* y *Honduras*.

De lo señalado en las tablas precedentes, se puede concluir que, bajo el enfoque de derechos a la intimidad y a la privacidad, se requiere mandato de ley para acceder, recopilar, proporcionar o divulgar datos personales en El Salvador, Venezuela, Chile y Brasil. Sin embargo, no existe uniformidad sobre qué elementos necesitan de autorización legal ni qué aspectos específicos requieren esta salvaguarda especial: datos personales de niñez y adolescencia o datos sensibles, por ejemplo. Desde otro lado, tampoco existe univocidad respecto de la recopilación, uso, tratamiento y cesión de datos personales que deben estar autorizados por ley y que, en consecuencia, no requieren autorización del titular, como por ejemplo, datos estadísticos, datos científicos, de interés general, necesarios para el ejercicio de competencias públicas, investigación de delitos o de infracciones administrativas, requeridos por orden judicial o por ser parte de procesos de contratación de servicios de terceros para tratamiento de datos; o aquellos que deben mantener una prohibición expresa que no admita excepciones.

Cabe señalar, además, que Paraguay, Honduras y Bolivia no contemplan en lo absoluto a la necesidad de mandato de ley para el tratamiento sin autorización del titular.

b) Respecto del derecho a la protección de datos personales

Se requiere mandato de ley para acceder, recopilar, proporcionar o divulgar datos personales para acciones y aspectos específicos, en los siguientes países:

Tabla 9

Tabla 9

País / Norma	Mandato legal	Principio de Libertad	Principio de acceso y circulación restringida	Acceder	Recopilar	Tratamiento	Anonimización o disociación	Proporcionar entre entes públicos	Divulgar entre entes públicos	Cedidos para cumplir con interés legítimo de cedente y cesionario.	Relativos a Niños, niñas y adolescentes	Finalidades no prohibidas	Datos sensibles
Argentina Ley 25326	SI, art. 5, num. 2, lit. b.	NO.	NO.	NO.	SI.	NO.	NO.	NO.	NO.	SI, art. 11, num. 3, lit. a).	NO.	NO.	SI, art. 7, LPDP. Solo pueden recolectar y tratar se datos sensibles cuando medien razones de interés general autorizados por ley.
Brasil	SI, art. 7 Artículo 7. El procesamiento de datos personales solo puede realizarse en los siguientes casos: I - otorgando el consentimiento del titular; II - para el cumplimiento de la obligación legal o reglamentaria por parte del controlador;(…)	NO	NO	SI, art. 18 LPDP	SI, art. 19 LPDP	SI, art. 7 LPDP	SI, art 5 numerales II y IX LPDP	SI, art. 22. LPDP	SI, art 23 LPDP menciona la difusión entre entes públicos.	SI, art. 7 numeral IX. LPDP	SI, art. 14 LPDP	NO	SI, art. 11 LPDP
Colombia Ley 1581	SI, art. 4, lit. a. Principio de legalidad: esta actividad es reglada y debe sujetarse obligatoriamente a lo dispuesto en la ley.	SI, art. 4, lit. c. Principio de libertad: los datos personales no podrán ser obtenidos o divulgados sin autorización previa, o en ausencia de mandato legal o judicial que releve el consentimiento.	SI, art. 4, lit. f. Principio de acceso y circulación restringida: el tratamiento se sujeta a los límites derivados de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. El tratamiento solo podrá hacerse por personas autorizadas por el titular y/o la ley, incluida su publicación en internet o medios masivos.	NO.	SI. Principio de legalidad, de libertad y de acceso y circulación restringida.	NO.	NO.	NO.	NO.	NO.	NO.	SI, art. 7. "Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública".	NO.	SI, art. 6. Los datos sensibles no pueden ser tratados a menos que exista disposición legal que lo autorice.
Ecuador	SI. Constitución de la República del Ecuador, Registro Oficial 449, 20 de octubre de 2008 (art. 66, núm. 19). La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.	NO.	NO.	NO.	NO.	NO.	NO.	SI, art. 49. Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. "No podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos".	SI, art. 49.- Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. "Las personas responsables de los bancos o archivos de datos personales únicamente podrán difundir la información archivada con autorización del titular o de la ley".	NO.	NO.	NO.	SI, art. 92. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias.
México	SI, art. 16, Constitución: será la ley la que establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos. Art. 18, LGTAIP: "El responsable podrá tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida".	SI, art. 16, Constitución. Especialmente el relativo al consentimiento en la recogida y tratamiento.	NO.	SI, art. 117, LFTAIP, reformada en 2017.	SI, art. 16, Constitución. Especialmente el relativo al consentimiento en la recogida y tratamiento.	SI, art. 16, Constitución. Especialmente el relativo al consentimiento en la recogida y tratamiento.	NO.	SI, art. 117, LFTAIP. "cuando se transmita entre sujetos obligados y entre éstos y los sujetos de derecho internacional, en términos de los tratados y los acuerdos interinstitucionales, siempre y cuando la información se utilice para el ejercicio de facultades propias de los mismo".					
Nicaragua	SI, art. 4, Ley de Protección de Datos: "será necesaria la autorización de la ley para la creación de ficheros de datos personales en los que no exista consentimiento del titular".	NO.	NO.	NO.	NO.	NO.	NO	NO.	NO.	NO.	NO.	NO.	SI, art. 8, Ley 787-2012. Los "datos sensibles sólo pueden ser obtenidos y tratados por razones de interés general en la Ley, o con el consentimiento del titular de datos, u ordenados por mandato judicial". Art. 17, lit. e). Ley 787-2012. El titular de los datos tiene derecho "a no ser obligada a proporcionar datos personales de carácter sensible, salvo las excepciones establecidas en la presente Ley".
Panamá	SI, art. 42, Constitución panameña. Toda persona tiene derecho a acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la ley. Esta información solo podrá ser recogida para fines específicos, mediante consentimiento de su titular o por disposición de autoridad competente con fundamento en lo previsto en la ley. Y el Art. 6 de la Ley 81.	NO.	NO.	SI.	SI.	SI.	SI, art. 3 Ley 81	NO.	NO.	Si, art. 8 numeral 9 Ley 81	NO.	NO.	Si, art. 8 numeral 9 Ley 81
Perú	SI, art. 13, núm. 2. Las limitaciones al ejercicio del derecho fundamental al derecho a la protección de datos personales solo podrán ser establecidas por ley, respetando su contenido esencial y justificarse en razón del respeto de otros derechos fundamentales. Art. 13, núm. 5. Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular,	NO.	NO.	NO.	NO.	NO.	SI, art. 14, núm. 8. "aplicando anonimización o disociación".	NO.	SI, art. 14, Ley 29733-2011 8. "1. cuando se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias".	NO.	SI, art. 13, núm. 3. "se necesita de reglamento que determine medidas especiales para el tratamiento de los datos personales de los niños y de los adolescentes".	NO.	SI, art. 13, núm. 6. "se necesita de ley para el tratamiento de datos sensibles, siempre que ello atienda a motivos importantes de interés público".

	salvo ley autoritativa al respecto.												
República Dominicana	SI. La Ley 172-13 recoge el principio de licitud por el cual los archivos de datos personales no pueden tener finalidades contrarias a las leyes o al orden público, siendo debidamente registrados y apegados a los principios establecidos en esta ley.					SI, art. 27. Las excepciones al consentimiento para el tratamiento y la cesión de datos están establecidas en esta norma de forma expresa.	Art. 27, núm. 9. "Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables".			SI, art. 27. Las excepciones al consentimiento para el tratamiento y la cesión de datos están establecidas en esta norma de forma expresa.			
Uruguay Ley 18.331	SI, art. 9. Determina que la regla es el consentimiento informado y que solo la información recogida cumpliendo con las características propias de este, puede ser considerada lícita. Art. 18.- Sobre datos sensibles pueden ser recolectados y tratados por razones de interés general autorizadas por ley, o si el organismo solicitante tiene mandato legal o si serán tratados con fines estadísticos.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	Art. 18. "Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, cuando el organismo solicitante tenga mandato legal para hacerlo".

Fuente y elaboración: La autora (2018).

En el mismo sentido, la recopilación, uso, tratamiento y cesión de datos personales se faculta por ley, aun sin autorización del titular, para casos o contextos específicos expresamente señalados, como los que constan a continuación:

Tabla 10

País / Norma	Fines históricos, estadísticos o científicos	Interés general	Interés vital del titular	Uso exclusivo, personal o doméstico	Salud física o mental	Salud pública, de emergencia, urgencia médica o sanitaria o para la realización de estudios epidemiológicos	Se limiten a nombre, documento de nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio	Datos de naturaleza pública	Registros públicos o accesibles al público	Datos relacionados con el Registro Civil de las Personas	Actividades legítimas por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical	Seguridad pública o nacional u orden público, fines de fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia	Ejercicio de competencias públicas, funciones legales, fines administrativos o autoridad pública o eficaz actividad ordinaria de la Administración	Adecuada prestación de servicios públicos	Investigación de delitos	Investigación de infracciones administrativas	Infracciones de la deontología en las profesiones	Reconocimiento, ejercicio o defensa de un derecho en un proceso judicial	Orden judicial	Contratación de servicios de terceros para tratamiento de datos	Producto de una relación contractual, científica o profesional del titular de los datos	Giro de las actividades comerciales o crediticias de los cesionarios	Operaciones que realicen las entidades financieras
Argentina Ley 25326	SI, art. 7, núm. 2 respecto de datos sensibles, "podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares".	SI, art. 7., LPDP. Solo pueden recolectar y tratar se datos sensibles cuando medien razones de interés general autorizados por la ley.	NO.	NO.	SI, art. 8. "Establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud [...] respetando los principios del secreto profesional".	SI, art. 11, num. 3, lit. d). "en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados".	SI, art.5, num. 2, lit. c). No será necesario consentimiento por mandato del citado artículo que señala expresamente a los listados de los datos personales generales.	NO.	NO.	NO.	SI, art. 7, núm. 3. La Iglesia católica, asociaciones religiosas, las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.	SI, art. 23, nums. 1, 2 y 3. "Para el estricto cumplimiento de sus misiones o para la represión de delitos y se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".	SI, art. 5, num. 2, lit. b); art. 11, num. 3, lit. c).	NO.	SI, Art. 7, nums. 1, 2 y 3 (datos sensibles: antecedentes penales y contravencionales). Art. 23, nums. 1, 2 y 3.	SI, art. 7, nums. 1, 2 y 3. Datos sensibles: antecedentes penales y contravencionales. Art. 23, nums. 1, 2 y 3.	NO.	NO.	NO.	NO.	SI, art. 5, num. 2, lit. d).	SI, art. 26, núm. 5. "La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios".	SI, art. 5, núm. 2, lit. e).
Brasil	SI, art. 7 IV – LGPD "(...) realizar estudios por parte del organismo de investigación, asegurando, siempre que sea posible, el anonimato de los datos personales (...)"	SÍ, art. 7 párrafo 3 LGPD "(...) El procesamiento de datos personales cuyo acceso es público considerará el propósito, la buena fe y el interés público que justificaron su disponibilidad. (...)"	NO	SI, art. 4 LGPD "(...) Esta Ley no se aplica al procesamiento de datos personales: I - realizado por una persona física con fines exclusivamente privados y no económicos. (...)"	SI, art. 7 IV – LGPD VII - "(...) para proteger la vida o la seguridad física del titular o de un tercero; VIII - para la protección de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridades de salud (...)"	NO	NO	NO	SI, art. 23 Párrafo 5. LGPD "(...) Los organismos notariales y de registro deberán proporcionar acceso a los datos por medios electrónicos a la administración pública, en vista de los fines mencionados en el contenido de este artículo. (...)"	NO	NO	SI, art. 4 LGPD	SI, Art. 7 numeral 3 LGPD	NO	SI, art. 4 literal d) LGPD	NO	NO	SI, art. 7 numeral VI LGPD	NO	NO	NO	SI, art. 7 numeral X LGPD - "(...) para la protección crediticia, incluidas las disposiciones de la legislación pertinente. (...)"	NO
Colombia Ley 1581	SI, art.10, lit. d); art. 6, lit. e). "El Tratamiento tenga una finalidad histórica, estadística o científica".	NO.	SI, art. 6, lit. b). Se prohíbe el tratamiento de datos sensibles, excepto por interés vital del titular y este se encuentre física o jurídicamente incapacitado.	NO.	NO.	SI, art. 10, lit. c).	NO.	SI, art.10, lit. b).	NO.	SI, art.10, lit. e).	SI, art.6, lit. c). Se prohíbe el tratamiento de datos sensibles excepto siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad".	NO. Revisar explicación al pie.	SI, art. 10, lit. a); art. 13, lit. b).	NO.	NO. Revisar explicación al pie.	NO. Revisar explicación al pie.	NO.	SI, art. 6, lit. d). Se prohíbe el tratamiento de datos sensibles excepto para procesos judiciales.	SI, art. 10, lit. a); art. 13, lit. b).	SI, art. 13, lit. c). "A los terceros autorizados por el Titular o por la ley".	NO. Existe normativa específica: Ley 1266 de 2008, por la cual se dicta disposiciones generales del *hábeas data* y se regula el manejo de información contenida en bases de datos personales, en especial la financiera, crediticia, comercial de servicios y la proveniente de terceros países.	

Costa Rica Ley n.º 8968	SI, art. 8, lit. d) "cuando no exista riesgo de que las personas sean identificadas".	NO.	SI, art. 9, num. 1, lit. a). Datos sensibles, prohibición de su tratamiento a menos que sea necesario para salvaguardar el interés vital del interesado o de otra persona.	NO.	NO.	SI, art. 9, num. 1, lit. d). "necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios".	NO.	NO.	SI, art. 9, num. 1, lit. c). Datos sensibles, prohibición de su tratamiento a menos que se refiera a datos que la persona interesada haya hecho públicos voluntariamente.	NO.	SI, art. 9, num. 1, lit. b). Datos sensibles, prohibición de su tratamiento a menos que sea actividades legítimas.	SI, art. 8, lit. b). Seguridad pública.	SI, art. 8, lit. b). Ejercicio de autoridad pública. Art. 8, lit. f). La eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales.	SI, art. 8, lit. e). La adecuada prestación de servicios públicos.	SI, art. 8, lit. c). La prevención, persecución, investigación, detención y represión de las infracciones penales.	NO.	SI, art. 8, lit. c). La prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones de la deontología en las profesiones.	SI, art. 9, num. 1, lit. c). Datos sensibles, prohibición de su tratamiento a menos que sean necesarios para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial.	NO.	NO.	NO, art. 8, núm. 4. Se regirán por las normas que regulan el Sistema Financiero Nacional.
Ecuador	NO.	NO.	NO.	NO.	NO.	Constitución de la República del Ecuador, en el art. 66, núm. 11, se reconoce el derecho a guardar reserva sobre sus convicciones, sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
México	NO.	NO.	NO.	NO.	NO.	Art. 16, Constitución. "seguridad y salud públicas o para proteger los derechos de terceros". Art. 4, LFPDPPP de 2010. "el orden, seguridad y salud públicas".	NO.	SI, art. 117, LFTAIP. "por ley tenga el carácter de pública".	SI, art. 117, LFTAIP. "registros públicos o fuentes de acceso público, o se requiera su publicación".	NO.	NO.	Art. 16, Constitución. "estas excepciones se fundarán exclusivamente en razones de seguridad nacional, disposiciones de orden público". Art. 117, LFTAIP, "seguridad nacional". Art. 4, LFPDPPP de 2010. "seguridad nacional". Art. 80, LGTAIP de 2015. "seguridad nacional, seguridad pública".	NO.	NO.	Art. 80, LGTAIP de 2015. "para la prevención o persecución de los delitos".	NO.	NO.	NO.	SI, art. 117, LFTAIP. "por orden judicial".	SI, art. 117, LFTAIP. "proteger los derechos de terceros". Art. 4 LFPDPPP de 2010. "derechos de tercero".	NO.
Nicaragua Ley 787-2012	SI, Art. 8. "datos sensibles sólo podrá tratarse con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares".	SI, art. 8, Ley 787-2012. "datos sensibles sólo pueden ser obtenidos y tratados por razones de interés general".	NO.	NO.	NO.	NO.	Art. 6, lit. d). "se obtengan de fuentes de acceso público irrestricto y se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, y fecha de nacimiento".	NO.	NO.	NO.	NO.	NO.	NO.	NO.	Art. 8. "datos sensibles relativos a los antecedentes penales o faltas administrativas sólo pueden ser tratados por las autoridades públicas competentes, en la esfera de sus competencias".	NO.	NO.	NO.	Art. 6, lit. a). "No será necesario el consentimiento cuando exista orden motivada, dictada por autoridad judicial competente".	NO.	Art. 6, lit.c). "tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable".
Panamá	SI, artículo 8 numeral 8 Ley 81, "(…) El tratamiento de información autorizado por	NO.	NO.	SI, art. 3 numeral 1 Ley 81 "(…) Los que realice una persona	NO.	SI, 7. artículo 8 numeral 7 Ley 81, "(…) Los casos de urgencia	SI, art. 8 numeral 4 Ley 81, "(…) Los que se contengan en listas relativas a una categoría de	NO.	SI; art. 8 numeral 1 Ley 81, "(…) Los que provengan o	NO.	SI, art. 3 numeral 4 Ley 81, "(…) Cuando se trate de tratamiento de datos relaciones con organismos	SI, art. 3 numeral 3 Ley 81, "(…) Los que se efectúen para el análisis de inteligencia	SI, art. 8 numeral 2 "(…) Los que se recolecten dentro del ejercicio de las funciones propias de la	NO.	SI, art. 3 numeral 2 Ley 81, "(…) Los que realicen autoridades competentes	NO.	NO.	NO.	NO.	NO	NO.	NO	SI, art. 8 numeral 3 Ley 81 "(…) Los de carácter económico, financiero,

	la Ley para fines históricos, estadísticos o científicos (…)" El artículo 8 numeral 6 Ley 81, "(…) El tratamiento de datos personales que realicen organizaciones privadas para el uso exclusivo de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otro de beneficio general de aquellos (…)"			natural para actividades exclusivamente personales o domésticas. (…)"		médica o sanitaria. (…)"		persona que se limiten a indicar antecedentes, como la pertenencia de la persona natural a una organización, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento (…)"		que se recolecten de fuentes de dominio público o accesible n medios públicos. (…)"		internacionales, en cumplimiento de lo dispuesto en los tratados y convenios vigentes ratificados por la República de Panamá (…)"	financiera y relativos a la seguridad nacional de conformidad con las legislaciones, tratados o convenios internacionales que regulen estas materias (…)"	Administración Pública en el ámbito de sus competencias (…)" El Art. 25. Dispone que: Los datos deberán ser mantenidos en formato interoperable y estructurado para el uso compartido, con miras a la ejecución de políticas públicas, a la prestación de servicios públicos, a la descentralización de la actividad pública ya la diseminación y el acceso de las informaciones por el público en general.		con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales (…)"					bancario o comercial que cuenten con el consentimiento previo (…)" 5. Art. 8 numeral 5 Ley 81 "(…) Los que son necesarios dentro de una relación comercial establecida, ya que sea para atención directa, comercialización o venta de los bienes o servicios pactados.(…)"		
Perú Ley 29733-2011	NO.	NO.	SI, art. 14, núm. 9. "Salvaguardar intereses legítimos del titular de datos personales".	NO.	NO.	SI, art. 14, núm. 6. "Relativos a salud y sea necesario en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular; cuando medien razones de salud pública; para la realización de estudios epidemiológicos o análogos, en tanto se aplique disociación".	NO.	NO.	SI, art. 14, Ley numeral 2. "Cuando estén contenidos o destinados a ser contenidos en fuentes accesibles para el público".	NO.	SI, art. 14, núm. 7. "Efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical sobre sus miembros".	NO.	SI, art. 14, núm. 1. "cuando se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias".	NO.	SI, art. 13, núm. 8. "se requiere norma expresa o convenio de encargo conforme la Ley Administrativa, para el tratamiento por parte de entidades públicas competentes relativos a la comisión de infracciones penales o administrativas".	NO.	NO.	SI, art. 13, núm. 4. "cuando se deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento".	SI, art. 13, núm. 4. "se requiere de mandamiento motivado del juez o autorización de su titular para abrir, incautar, interceptar o intervenir comunicaciones, telecomunicaciones, sistemas informáticos o sus instrumentos".	SI, art. 14, núm. 5. "cuando sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte".	SI, art. 14, núm. 5. "cuando se traten de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento".	SI, art. 14, núm. 3. "Relativos a solvencia patrimonial y de crédito s".	SI, art. 14, núm. 4. "Medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos regulados por la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privadas en los servicios Públicos, o la que haga sus veces".
República Dominicana	NO.	NO.	NO.	NO.	NO.	Art. 27, núm. 8. "Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve el secreto de la identidad de los titulares de los datos mediante mecanismos de disociación	Art. 27, núm. 3. "Se trate de listas para fines mercadológicos, cuyos datos se limiten a nombre, cédula de identidad y electoral, pasaporte, identificación tributaria y demás informaciones biográficas".	NO.	Art. 27, núm. 1. "Se obtengan de fuentes de acceso público".	NO.	NO.	NO.	Art. 27, núm. 2. "Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal". Art. 27. 7. "Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias".	NO.	NO.	NO.	NO.	NO.	NO.	Art. 27, núm. 4. "Se deriven de una relación comercial, laboral o contractual".	Art. 27, núm. 4. "Se deriven de una relación comercial, laboral o contractual, científica o profesional con la persona física, y resulten necesarios para su desarrollo o cumplimiento".	Art. 27, núm. 5. "Se trate de datos personales que reciban de sus clientes en relación a las operaciones que realicen las entidades de intermediación financiera reguladas por la Ley Monetaria y Financiera y de agentes económicos, de las Sociedades de Información Crediticia (SIC), y de las entidades que desarrollan herramientas de puntajes de crédito para la evaluación del riesgo de los deudores del sistema financiero y comercial nacional".

					adecuados".																
Uruguay Ley 18.331	SI, art. 18. Los datos sensibles "También podrán ser tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares".	Art. 18. Sobre datos sensibles pueden ser recolectados y tratados por razones de interés general.	NO.	SI, art. 9, lit. d. "Se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico".	SI, art. 19. "Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional".	NO.	SI, art. 9, lit. c). "Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma".	NO.	SI, art. 9, lit. a) "Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación".	NO.	SI, art. 18. "aquellos que posean los partidos políticos, sindicatos, iglesias, confesiones religiosas, asociaciones, fundaciones y otras entidades sin fines de lucro, cuya finalidad sea política, religiosa, filosófica, sindical, que hagan referencia al origen racial o étnico, a la salud y a la vida sexual, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio que la comunicación de dichos datos precisará siempre el previo consentimiento del titular del dato".	NO.	SI, art. 9, lit. b). "Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".	NO.	SI, art. 18. "Los datos personales relativos a la comisión de infracciones penales, civiles o administrativas sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes".	SI, art. 18. "Los datos personales relativos a la comisión de infracciones penales, civiles o administrativas sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes".	NO.	NO.	NO.	NO.	SI, art. 9, lit. d. "Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento".	Los artículos 21 y 22 señalan: Datos de bases de datos con fines de publicidad y relativos a la actividad comercial o crediticia. Queda expresamente autorizado el tratamiento de datos personales destinados a brindar informes objetivos de carácter comercial, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor o en las circunstancias previstas en la presente ley.

Fuente y elaboración: La autora (2018).

A continuación, constan los casos de Colombia y México que sobre el tema desarrollan contenido específico que debe explicarse.

Colombia establece una peculiaridad, ya que no le será aplicable el régimen de protección de datos personales a las bases de datos o archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo o que contengan información de inteligencia y contrainteligencia. Asimismo, las bases de datos y archivos de información periodística y otros contenidos editoriales relativos a censos de población y vivienda, Ley 79 de 1993 y aquella financiera, crediticia y comercial, Ley 1266 de 2008. Ahora bien, los principios sobre protección de datos le serán aplicables pese a que la normativa especial regule en consideración a la naturaleza especial de estos datos, y deberán aplicarse de forma concurrente.

México, llama la atención la figura que consta en el artículo 117, LFTAIP, que aplica a la excepción relativa a razones de seguridad nacional y salubridad general, o para proteger los derechos de terceros, se requiera su publicación, por la cual el Instituto deberá aplicar la "prueba de interés público, que consiste en corroborar una conexión patente entre la información confidencial y un tema de interés público y la proporcionalidad entre la invasión a la intimidad ocasionada por la divulgación de la información confidencial y el interés público de la información".

Finalmente, como conclusión del estudio de este elemento del contenido esencial se colige que todas las legislaciones, tanto aquellas enfocadas en derechos de intimidad y privacidad, como aquellas que salvaguardan datos personales como derecho, coinciden que la piedra angular del sistema de protección es el consentimiento, y que, en su ausencia debe existir disposición legal u orden judicial que interprete la ley que autorice su tratamiento.

Además, se puede avizorar que aquellos países que han desarrollado normativas especializadas en protección de datos personales coinciden en determinar como elemento esencial a la mención expresa de la necesidad de mandato legal para el acceso, recopilación, tratamiento, divulgación y cesión sin autorización del titular, aunque no existe uniformidad sobre los términos empleados, pues en varios países basta la mención a la recopilación o al tratamiento.

Asimismo, Colombia desarrolla tres principios relacionados que ayudan a completar la configuración de la necesidad de mandato legal para el tratamiento sin autorización del titular como: el principio de legalidad, el principio de libertad y el principio de acceso y circulación restringida.

La anonimización y la disociación, como técnicas de protección de datos, además de medidas de seguridad se interpretan como elementos que, implantados en los datos personales, permiten su difusión.

Aparece como necesidad inicial que los datos personales puedan ser proporcionados o divulgados entre entes públicos, tanto para el cumplimiento de las competencias públicas, funciones legales, fines administrativos o autoridad pública para garantizar una adecuada o eficaz actividad ordinaria de la Administración o servicio público.

Otra condición autorizada por ley, es aquella en la que se cede para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario, entre los que constan las relaciones precontractuales y contractuales.

Finalmente, casos especiales como los relativos a niños, niñas y adolescentes y a datos sensibles que tienen un tratamiento diferenciado generalmente autorizado cuando están disociados o anonimizados los datos.

Entre los países analizados, son casos comunes que autoriza la ley tratar aun sin autorización del titular los siguientes: finalidades históricos, estadísticos o científicos, siempre que estén disociados o anonimizados los datos, casos sobre salud física o mental, de salud pública, de emergencia, urgencia médica o sanitaria o para la realización de estudios epidemiológicos; aquellos que se limiten a nombre, documento de nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; los datos de naturaleza pública; los de registros públicos o accesibles al público, o relacionados con el Registro Civil de las Personas; aquellos necesarios para actividades legítimas por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical. También, sobre seguridad pública o nacional u orden público, fines de fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; necesarios para la investigación de delitos, infracciones administrativas o infracciones de la deontología en las profesiones; el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; por orden judicial; contratación de servicios de terceros para tratamiento de datos; producto de una relación contractual, científica o profesional del titular de los datos, el giro de las actividades comerciales o crediticias de los cesionarios; las operaciones que realicen las entidades financieras.

Si bien, Argentina, Uruguay y Nicaragua usan la expresión “interés general”, esta resulta vaga por lo que es preferible una determinación taxativa de los casos en los que procede el tratamiento por autorización legal. Se anota, además, que Perú establece que las limitaciones al ejercicio del derecho fundamental al derecho a la protección de datos personales solo podrán ser establecidas por ley, respetando su contenido esencial y justificarse en razón del respeto de otros derechos fundamentales.

Asimismo, Colombia, Costa Rica y Perú consideran necesario incluir la expresión “interés vital” del titular aun cuando señalan casos relacionados a la salud.

Finalmente, la legislación uruguaya y la panameña incluyen al “uso exclusivo, personal o doméstico” como datos de los cuales se exime del consentimiento o se exime del ámbito de protección de la ley, respectivamente. En este último caso, también la normativa brasileña hace referencia al “realizado por una persona física con fines exclusivamente privados y no económicos” De esta manera se evidencia que este tipo de tratamiento de datos no justifica un régimen de protección.

De lo dicho, se utilizan términos similares, expresiones más o menos comunes y claras para establecer casi los mismos casos por los cuales la ley releva la autorización del titular. En general estos casos son relativos al interés general, relaciones con el Estado, entre particulares motivados en la entrega de servicios y casos especiales de datos especialmente protegidos.

Mientras que aquellos que eximen de aplicación a la normativa de protección de datos son los referentes a información periodística, datos anonimizados, a aquellos de uso personal o doméstico; propiedad intelectual, secretos profesionales, secretos industriales, o la investigación de delitos.

1.5.4 Principios

1.5.4.1 Deber de información

a) Respecto del derecho a la intimidad y a la privacidad:

Desde esta perspectiva, se colige lo siguiente:

Tabla 11

País	Deber de información	Derecho de información
El Salvador	NO.	NO.
Venezuela	El artículo 78 de la Ley de Infogobierno señala que para el caso de registro de datos de niños, niñas y adolescentes el receptor de los datos debe priorizar e indicar los derechos que le asisten y la normativa aplicable para llevar a cabo el trámite solicitado en beneficio del niño, niña o adolescente, es decir un deber de información general y específico en garantía de este grupo vulnerable.	El artículo 28 de la Constitución, referente básico en este análisis, no hace mención alguna a los principios del derecho a la protección de datos personales. Cuando habla de información lo hace desde la perspectiva del derecho de información no desde la obligación del responsable del fichero de entregar esta so pena de recibir algún tipo de asignación de responsabilidad o sanción.
Bolivia	NO. En el artículo 30 de la Constitución aparece de manera referencial la negativa de dar a conocer datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, de producirse se considera indebida e ilegal. Respecto al Decreto Supremo 1793, en el artículo 4, aplicable a quienes brinden servicios de certificación digital se establece el principio de transparencia, por el cual, cuando traten de datos personales deberán garantizar al titular en cualquier momento y sin impedimento alguno la información relacionada de la existencia de los datos que le conciernan. Su aplicación es limitada a las entidades certificadoras por lo que este criterio sectorial es meramente orientativo. Lo mismo respecto del artículo 56 que dice que las personas titulares deberán ser "previamente informadas de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de éstos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes".	
Chile	NO.	
Honduras	NO.	
Paraguay	NO. Respecto del deber que tienen los responsables de los	Ahora bien, como los titulares gozan del derecho de información, en contrario

	ficheros oficiales o privados de carácter público no existe una expresión específica en la norma constitucional (art. 35, Constitución de la República de Paraguay).	sentido, es propio un deber de información por parte de los responsables de los ficheros que permita la efectividad de este derecho aunque no conste expresamente reconocido en la normativa.

Fuente y elaboración: La autora (2018).

Del análisis de la tabla 11, se concluye que aquellos países en los cuales se reconoce el derecho a la intimidad, como base para la protección de los datos personales, aparece el derecho de información del titular, mas no necesariamente el deber de información que deben cumplir los responsables del tratamiento.

Por ello, El Salvador, Chile, Honduras y Paraguay no contemplan el deber de información. En el caso de Bolivia, lo contempla pero limitado a quienes brinden servicios de certificación digital, operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación.

Solo Venezuela y Paraguay consideran al deber de información como un derecho. En el caso de Venezuela, y respecto de niños, niñas y adolescentes, se solicita que el receptor de los datos priorice e indique los derechos que le asisten y la normativa aplicable para llevar a cabo el trámite solicitado en beneficio del niño, niña o adolescente (art. 78, Ley de Infogobierno).

b) Respecto del derecho a la protección de datos personales

Al respecto, se considera que:

Tabla 12

País	Deber de información	Sin barreras técnicas que impidan su acceso	Sobre que se informa												
			Finalidad	Motivos	Destinatarios	Tipo de tratamiento	Cesión	Existencia del archivo	Identidad responsable	Domicilio responsable	Carácter obligatorio o facultativo de las respuestas	Consecuencias	Derechos	Tiempo	Avisos de privacidad
Argentina	El artículo 6 de la Ley de Protección de Datos Personales señala que cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara sobre los asuntos que se detallan expresamente en la norma.	NO.	SI. Art. 6, lit. a). "La finalidad para la que serán tratados los datos..."	NO.	SI. Art. 6, lit. a). "quiénes pueden ser sus destinatarios o clase de destinatarios".	NO.	NO.	SI. Art. 6, lit. B). "La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate".	SI. Art. 6, lit. b). "la identidad y domicilio de su responsable..."	SI. Art. 6 literal b) "(...) la identidad y domicilio de su responsable".	SI. Art. 6, lit. c) "El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga".	SI. Art. 6, lit. d). "Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos..."	SI. Art. 6, lit. e). "La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. Es decir, de las condiciones básicas para el ejercicio de los derechos que permiten la efectiva vigencia de este derecho fundamental...".	NO.	NO.
Brasil	El derecho de información aparece como principio de transparencia en el artículo 6, 9 y 18 de la LGPD por el cual los datos	NO	SI, art. 9 numeral I LGPD "(...) - propósito específico del tratamiento; (...)"	NO	SI art.18 numeral VII LGPD "(...)- información sobre entidades públicas y privadas con	SI art.18 numeral I LGPD "(...) confirmación de la existencia de tratamiento (...)"	SI art. 9 numeral V LGPD "(...) información sobre el uso compartido de datos por el controlador y el	NO	SI art. 9 numeral III LGPD "(...) identificación del controlador (...)"	SI art. 9 numeral IV LGPD "(...)- información de contacto del controlador (...)"	SI art.18 numeral VIII LGPD "(...) información sobre la posibilidad de no dar consentimien	NO	SI art. 9 numeral VII LGPD "(...) derechos del titular, con mención explícita de los derechos contenidos en	SI art. 9 numeral II LGPD "(...) forma y duración del tratamiento,	NO

	personales deben estar “disponibles de manera clara, apropiada y abierta” (artículo 9 de la LGPD)				las cuales el controlador hizo uso compartido de datos (…)”	SI art. 9 numeral II LGPD “(…) forma y duración del tratamiento,	propósito (…)”				to y sobre las consecuencias del rechazo (…)”		el art. 18 de esta Ley (…)”	observando los secretos comerciales e industriales (…)”	
Colombia	Art. 12, Ley 1581 de 2012. Deber de informar al Titular. “El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa”.	SI. Art. 11, Ley 1581 de 2012. “obligación del titular de las bases de datos de suministrar la información por cualquier medio, incluyendo los electrónicos, a petición del Titular. Esta obligación incluye que sea completa, de fácil lectura, sin barreras técnicas que impidan su acceso”.	Art. 12, lit. a), Ley 1581 de 2012. “El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo”.								Art. 12, Ley 1581 de 2012. “d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento…”	Art. 12, Ley 1581 de 2012. “b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes. ..”	Art. 12, Ley 1581 de 2012. “c) Los derechos que le asisten como Titular…”		
Costa Rica	Incluido dentro del consentimiento. De acuerdo con el artículo 5 de la Ley 8968 y dentro del principio de consentimiento informado consta la obligación de informar, cuando se soliciten datos de carácter personal a su titular o representante de modo expreso en lo	Art. 5. “Incluyendo también que en caso de utilizar cuestionarios u otro medio de recolección de datos personales, deben figurar los mencionados puntos en forma claramente legible”.	SI. Art. 5. “los fines que se persiguen con su recolección… ”	NO.	SI. Art. 5. “los destinatarios y quienes podrán consultar la información… ”	SI. Art. 5. “el tratamiento que se aplicará…”	NO.	SI. Art. 5. “la existencia de una base de datos personal…”	SI. Art. 5. “la identidad…”	SI. Art. 5. “dirección de quien asume responsabilidad sobre la base de datos…”	SI. Art. 5. “del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección… ”	SI. Art. 5. “las consecuencias de la negativa a suministrarlos…”	SI. Art. 5. “la posibilidad de ejercer derechos…”	NO.	NO.

	relacionado a...												
Ecuador		NO.											
Guatemala	Limitado a capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos.	Pero en el artículo 31 de la misma ley consta la obligación tomar el consentimiento para la difusión, distribución o comercialización de los datos, evitando incurrir en un vicio de la voluntad y por lo tanto aparece la obligación de explicar claramente las consecuencias de sus actos. De esta forma, se entiende que existe un deber de información que garantice una voluntad libre de vicios.											
México	Art. 15, Ley federal de protección de datos personales en posesión de los particulares. "El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad". Art. 16. El aviso de privacidad deberá contener, al menos...	Art. 17, LFPDPPP. "El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología". Art. 26, LGPDPPSO. Por regla general, el aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente el responsable. Para que el aviso de privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara y	Art. 15, LFPDPPP. "la información que se recaba de ellos y con qué fines, a través del aviso de privacidad". Art. 16, LFPDPPP. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular. Art. 28, LGPDPPSO. IV. Las finalidades	NO.	NO.	Art. 26, LGPDPPSO. El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. Art. 27, LGPDPPSO. "Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular".	Art. 15, LFPDPPP. "En su caso, las transferencias de datos que se efectúen..." Art. 27, LGPDPPSO. "Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar: a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y b) Las finalidades de estas transferencias...	NO.	Art. 15, LFPDPPP. "La identidad y domicilio del responsable que los recaba..." Art. 27, LGPDPPSO. "La denominación del responsable..."	Art. 15, LFPDPPP. "La identidad y domicilio del responsable que los recaba..." Art. 28, LGPDPPSO. "El domicilio del responsable..."	NO.	NO.	Art. 15, LFPDPPP. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los derechos. Por regla general, el aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente el responsable. Art. 27, LGPDPPSO. "Los mecanismos y medios disponibles para que el titular, en	NO.	Art. 15, LFPDPPP. "información que se recaba de ellos y con qué fines, a través del aviso de privacidad". Art. 16, LFPDPPP. El aviso de privacidad deberá contener, al menos el procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta ley. En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos. Art. 3, LGPDPPSO. Aviso de privacidad: Documento a disposición del titular de forma

		sencilla.	del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular.			Art. 28, LGPDPPSO. "II. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles [...] III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento".	"						su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular, y V. El sitio donde se podrá consultar el aviso de privacidad integral. Art. 28, LGPDPPSO. "V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO. VI. El domicilio de la Unidad de Transparencia, y VII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad".		física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos. Art. 27, LPDPSO. El aviso de privacidad a que se refiere el artículo 3, fracción II, se pondrá a disposición del titular en dos modalidades: simplificado e integral. El aviso simplificado deberá contener la siguiente información: I. La denominación del responsable; II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular.
Nicaragua	Art. 7, Ley de Protección de Datos Personales. El deber que tienen los responsables de los ficheros de informar a los titulares de los datos de los datos que tienen registrados.	NO.	SI. Art. 7. "las finalidades de sus usos..."	SI. Art. 7. "los motivos de la recogida..."	NO.	SI. Art. 7. "los tratamientos a los que ha sido sometidos los datos..."	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO

Panamá	El artículo 6 de la Ley 81 establece como elemento condicional para que el consentimiento sea efectivo que, la persona sea "debidamente informada respecto del propósito del uso de sus personales".	NO	SI, art. 6 de la Ley 81 "(…) informada respecto del propósito del uso de sus personales (…)".	NO	NO	NO	NO	NO	NO	NO	NO	Art. 2 numeral 6 Ley 81 "(…) mantenerlo informado de todos los derechos que le amparan como titular del dato, así como la posibilidad de ejercer los derechos ARCO (…)"	NO	NO	
Perú	Art. 18, Ley de Protección de Datos Personales de 2011. El deber de informar al titular del dato.	SI "El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación…"	SI. Art. 18. "Sobre la finalidad para la que sus datos personales serán tratados…"	NO.	SI. Art. 18. "Quiénes son o pueden ser sus destinatarios. .."	NO.	SI. Art. 18. "La transferencia de los datos personales…"	SI. Art. 18. "la existencia del banco de datos en que se almacenará n…"	SI. Art. 18. "así como la identidad y domicilio de su titula y, de ser el caso, del encargado del tratamiento de sus datos personales…"	SI. Art. 18. "así como la identidad y domicilio de su titula y, de ser el caso, del encargado del tratamiento de sus datos personales…"	SI. Art. 18. "El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles…"	SI. Art. 18 "Las consecuencia s de proporcionar sus datos personales y de su negativa a hacerlo…"	SI. Art. 18. "La posibilidad de ejercer derechos que la ley le concede y los medios previstos para ello…"	SI. Art. 18. "El tiempo durante el cual se conserven sus datos personale s…"	SI. Art. 18. "Si los datos personales son recogidos en línea a través de redes de comunicacione s electrónica, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que debe ser fácilmente accesibles e identificables.. ."

República Dominicana	Art. 5, Ley 172-13. "Derecho de información. Cuando se recaben datos personales que requieran del consentimiento del titular de los datos..."	NO.	SI Art. 5, Ley 172-13. "para que se les pueda dar el tratamiento de datos: a) La finalidad para la que serán destinados y quiénes pueden ser sus destinatarios o clase de destinatarios ..."	NO.	NO.	NO.	SI. Art. 5, Ley 172-13. "o ser cedidos después de obtener dicho consentimiento, se deberá informar previamente, a por lo menos uno de los titulares de los datos, en forma expresa y clara, explicando..."	SI. Art. 5, Ley 172-13. "b) La existencia del archivo, registro, banco de datos o de cualquier otro tipo de que se trate..."	SI. Art. 5, Ley 172-13. "y la identidad y domicilio de su responsable..."	SI. Art. 5, Ley 172-13. "y la identidad y domicilio de su responsable..."	NO.	NO.	SI. Art. 5, Ley 172-13. "c) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos..."	NO.	NO.
Uruguay	El artículo 13 de la Ley de Protección de Datos Personales dice que cuando se describe el derecho de información se determina que los responsables deberán informar previamente. El Decreto 414/009 señala la obligación para recolección del consentimiento informado.	SI. Art. 13. "titulares en forma expresa, precisa e inequívoca..."	SI. Art. 13 "(...) la finalidad Art. 5 del Decreto 414/009 dice: "(...) se solicita que se conozca inequívocamente la finalidad a la que se destinarán los datos (...)".	NO.	SI. Art. 13. "destinatarios de los datos tratados..."	SI. Art. 13. "tratamiento de datos..." Art. 5, Decreto 414/009. "es decir que y el tipo de actividad desarrollada por el responsable de la base de datos o tratamiento. En caso contrario, el consentimiento será nulo..."	NO.	SI. Art. 13. "la existencia de la base de datos cualquiera sea su soporte..."	SI. Art. 13. "la identidad; el domicilio del responsable..."	SI. Art. 13. "la identidad; el domicilio del responsable..."	SI. Art. 13. "el carácter obligatorio o facultativo de las respuestas, especialmente datos sensibles..."	SI. Art. 13. "las consecuencias de entregar o no sus datos..."	SI. Art. 13. "los derechos de acceso, rectificación y supresión de datos de los cuales son titulares..."	NO.	NO.

Fuente y elaboración: La autora (2018).

Acerca de los países que sustentan el sistema de salvaguarda de los datos personales sobre la concepción de un derecho de protección de estos, se evidencia que la mayoría recoge el deber de información, excepto aquellos que no tienen norma específica que la desarrolle, como Guatemala, Ecuador y Panamá.

Por el contrario, el resto de países que tienen normativa especializada opta por concebirlo como derecho y también como deber, y considerarlo entre sus principios; desarrollan pormenorizadamente las características y peculiaridades de la entrega de información con excepción de Colombia en cuyo literal e) del artículo 4º de la Ley 1581 de 2012, Ley de Protección de Datos Personales, establece la obligación de que el Gobierno nacional establezca la forma en la cual los responsables y encargados del tratamiento suministren la información del titular, dejando al organismo público la determinación de tales condiciones.

Los países que legislan sobre la necesidad de que no existan barreras técnicas que impidan su acceso a la información son Colombia, Costa Rica México, Perú y Uruguay.

Perú, Panamá y México establecen la necesidad de trabajar con avisos de privacidad mediante los cuales se pretende desarrollar el deber de información.

Otros consideran que el deber de información no se limita a realizar a los avisos de privacidad disponibles en sitios o plataformas web sino que debe realizarse de forma expresa en cada interacción y canal existente entre el titular del dato y el responsable, por ello se establece una serie de informaciones y condiciones que deben ser entregadas al titular.

Ya sea que se usen avisos de privacidad o no, la mayoría de legislaciones informa sobre:

- *La finalidad del uso de los datos personales:* Argentina, Brasil, México, Colombia, Costa Rica, Nicaragua, Panamá Perú, República Dominicana y Uruguay.
- *Los motivos del tratamiento:* únicamente Nicaragua determina la obligación de informar sobre los motivos de la recogida.
- *Los destinatarios de los datos personales:* Sobre quiénes pueden ser sus destinatarios o clase de destinatarios que pueden consultar estos datos legislan Argentina, Costa Rica, Perú y Uruguay. En el caso de Brasil, se determina la necesidad de informar sobre las entidades públicas y privadas con las cuales el controlador hizo uso compartido de datos, de esta manera se informa la identidad de los destinarios de los datos personales.
- *Los tipos de tratamiento:* por medio del aviso de privacidad, o de forma directa se deberá informar sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto conforme señalan legislaciones como la de Colombia, México, Costa Rica, Nicaragua y Uruguay. En el caso del Brasil, además se debe entregar información sobre la existencia de un tratamiento.
- *La cesión o transferencia de datos:* México, Perú y Uruguay. En el caso del Brasil no solo se informa sobre el uso compartido de datos por parte del controlador (responsable de tratamiento) sino además del propósito de dicha cesión.

- *La existencia del archivo, base de datos, electrónico o de cualquier otro tipo de que se trate:* Argentina, Costa Rica, Perú, República Dominicana y Uruguay.
- *La identidad del responsable:* Argentina, Brasil, México, Costa Rica, Perú, República Dominicana y Uruguay.
- *El domicilio responsable:* Argentina, Brasil, México, Colombia, Costa Rica, Perú, República Dominicana y Uruguay.
- *El carácter obligatorio o facultativo de las respuestas:* Argentina, Brasil, Colombia, Costa Rica, Perú y Uruguay.
- *Las consecuencias del tratamiento de los datos:* Argentina, Costa Rica, Perú y Uruguay.
- *Los derechos que poseen los titulares y las formas efectivas de ejercerlos:* Argentina, Brasil, Colombia, México, Costa Rica, República Dominicana, Panamá, Perú y Uruguay.
- Anotándose que en el caso de México que utiliza avisos de privacidad y establece la obligación de difundir por medios electrónicos y físicos los mecanismos y medios disponibles para que el titular pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular, y además el sitio donde se podrá consultar el aviso de privacidad integral.
- *El tiempo de vigencia de los datos personales en poder del responsable:* Brasil y Perú establecen el deber de información sobre esta temática.
- *La necesidad de implementar avisos de privacidad, especialmente mediante medios electrónicos:* México (dos modalidades: simplificado e integral) y Perú son los dos únicos países que utilizan esta figura.

1.5.4.2 Pertinencia

a) Respecto del derecho a la intimidad y a la privacidad

Desde esta perspectiva, se colige lo siguiente:

Tabla 13

	Elementos que configuran la pertinencia		
País	**Seguridad**	**Actualización**	**Adecuados o proporcionales**
El Salvador	NO.	NO.	NO.
Bolivia	NO.	NO.	NO.
Chile	NO.	NO.	NO.
Honduras	NO.	NO.	NO.
Paraguay		Pertinencia entendida como consecuencia directa de la actualización de los datos personales. El artículo 7° de la Ley 1682 de 2001 al establecer la obligación de los responsables de los registros de actualizar permanentemente los datos personales sobre situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales para que de acuerdo con la ley puedan difundirse o publicarse,	

	señala que las empresas, personas o entidades que utilizan los servicios de las entidades que los difunden tengan la obligación de suministrarles la información pertinente a fin de que los datos que aquellas almacenen, procesen y divulgue, se hallen permanentemente actualizados.	
Venezuela		La Ley de Infogobierno señala en el artículo 22 del capítulo II, Principios y bases del uso de las tecnologías de información, el principio de proporcionalidad que determina que en las actuaciones que realicen el Poder Público y el Poder Popular a través de las tecnologías de información, solo se exigirán a las personas los datos que sean estrictamente necesarios para tramitar los asuntos que haya solicitado, a los fines de garantizar el cumplimiento de los principios y derechos establecidos en la Constitución de la República y la ley.

Fuente y elaboración: La autora (2018).

Según se desprende de la tabla 13, El Salvador, Bolivia, Chile, Honduras no mencionan al principio de pertinencia ni formas similares. Solo tres países incluyen de forma indirecta el principio de pertinencia: Brasil, Paraguay y Venezuela.

Por su parte, Paraguay considera a la pertinencia como el criterio por el cual se efectiviza la obligación de actualizar los datos por parte de los responsables del tratamiento. Finalmente, Venezuela al describir el principio de proporcionalidad recoge una aproximación al principio de pertinencia, cuando señala que solo se exigirán a las personas los datos que sean estrictamente necesarios para tramitar los asuntos que haya solicitado, aunque su ámbito de aplicación es limitado al sector público.

b) Respecto del derecho a la protección de datos personales

Al respecto se considera que:

Tabla 14

País	Normativa	Contenido en el principio de calidad	Contenido en otros principios	Cierto Correcto Veraz	Adecuado o pertinente	Exacto	Completo	Actualizado	Necesario	No excesivos en relación al ámbito	No excesivos en relación a la finalidad	No excesivos para su propósito de recogida	Si han dejado de ser pertinentes deben destruirse
Argentina	Los numerales 1 y 7 del artículo 4, LPDP, señalan que los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido y en el caso de que estos hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados deberán ser destruidos.	SI.	NO.	SI.	SI.	NO.	NO.	NO.	NO.	SI.	Numerales 1 y 7 del artículo 4, LPDP. "y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido..."	NO.	SI.
Brasil	Artículo 6 de la LGPD II "(...) adecuación: compatibilidad del tratamiento con los fines informados al propietario, según el contexto del tratamiento (...)	NO	NO.	NO.	SI	NO.	NO.	NO.	NO.	SI, en relación al contexto del tratamiento...	SI. Compatibilidad con los fines	SI. Con los fines informados	NO
Colombia	NO.	Aunque no existe mención expresa en ninguna de las dos normas analizadas, sin embargo, podemos colegir que su aplicabilidad se manifiesta por medio de otros principios como el de calidad y el de finalidad de los datos.	Aunque no existe mención expresa en ninguna de las dos normas analizadas, sin embargo, podemos colegir que su aplicabilidad se manifiesta por medio de otros principios como el de calidad y el de finalidad de los datos.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Costa Rica	El artículo 6 de la Ley 8968, sobre la exactitud de los datos, señala que la persona responsable de la base de datos tomará las medidas necesarias para que los datos sean exactos y completos, con respecto a los fines para los que fueron	SI.	NO.	NO.	NO.	SI.	SI.	NO.	NO.	NO.	Artículo 6, Ley 8968. "Pertinentes con los fines para los que fueron	NO.	NO.

	recogidos o para los que fueron tratados posteriormente.										recogidos o para los que fueron tratados posteriormente. .."		
Ecuador	NO.												
Guatemala	Decreto 57-2008, Ley de Acceso a la Información Pública. En el artículo 30, numeral 2, al referirse al *habeas data* se señala que los sujetos tendrán la responsabilidad de que los datos almacenados sean adecuados, pertinentes y no excesivos, en relación con los propósitos para los cuales se hayan obtenido.	NO.	Contenido en el *habeas data*.	NO.	SI.	NO.	NO.	NO.	NO.	NO.	NO.	SI.	NO.
México	Artículo 11, LPPDPP. El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	SI. Artículo 6, LPPDPP.	NO.	SI.	NO.	NO.	NO.	SI.	NO.	NO.	Artículo 11, LPPDPP. "sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados..."	NO.	Artículo 11, LPPDPP. "Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados".
Nicaragua	El artículo 19 de la LOPD, en el derecho de cancelación, señala su procedencia cuando los datos han dejado de ser necesarios o pertinentes para la finalidad que dio lugar a su tratamiento.	NO.	En el derecho de cancelación.	NO.	NO.	NO.	NO.	NO.	SI.	NO.	NO.	NO.	Deben cancelarse cuando han dejado de ser pertinentes.
Panamá	NO	NO	El artículo 2, numeral 3 Ley 81.- Principio de proporcionalidad: solo deberán ser solicitados aquellos datos adecuados, pertinentes y limitados al mínimo necesario en relación con la finalidad para la que son requeridos	NO	SI	NO	NO	NO	NO	NO	SI	NO	NO
Perú	Artículo 8, Ley 29733. "Principio de Calidad: Los datos personales que vayan a ser tratados deber ser veraces, exactos y, en la medida de lo posible, actualizada, necesaria, pertinente y adecuada respecto de la finalidad para la que fueron recopilados..."	SI.	NO.	SI. Veraz.	SI.	SI.	NO.	SI. En la medida de lo posible actualizado.	SI.	NO.	Art. 8, Ley 29733. "respecto de la finalidad para la que fueron recopilados..."	NO.	Art. 8, Ley 29733. "Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con su finalidad del tratamiento".

República Dominicana	El artículo 5, numeral 2, de la Ley 172-13 recoge el principio de calidad de los datos, por el cual: a) Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados y pertinentes en relación al ámbito y finalidad para los que se hubieren obtenido; b) Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario…"	SI.	NO.	SI.	SI.	SI.	NO.	SI.	NO.	SI.	Art. 5, núm. 2, Ley 172-13. "adecuados y pertinentes en relación al ámbito y finalidad para los que se hubieren obtenido…"	NO.	Art. 5, núm. 2, Ley 172-13. "c) Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o, en su caso, completados por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate".
Uruguay	Artículo 8º, Ley 18.331. "Principio de finalidad.- Los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención".	NO.	Principio de finalidad.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	Art. 8º, Ley 18.331. Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados.

Fuente y elaboración: La autora (2018).

Sobre el principio de pertinencia, ninguno de los países analizados lo consagra como principio autónomo, sino que consta como parte del principio de calidad: Argentina, Costa Rica, México, Perú y República Dominicana. O en el caso de Panamá que lo integra al principio de proporcionalidad.

Brasil lo concibe como el principio de adecuación, por el cual determina el alcance de la pertinencia asociado a la finalidad del tratamiento y no a la calidad del dato, por cuanto señala que se producirá cuando exista compatibilidad entre el tratamiento de los datos personales y su respectivo contexto, con las finalidades informadas al titular.

Uruguay lo considera parte del principio de finalidad. Colombia colige la pertinencia de la aplicabilidad de los principios de finalidad y calidad de datos; y Guatemala como parte del *habeas data*.

Finalmente, Nicaragua lo incluye en el derecho de cancelación cuando obliga a eliminar el contenido que ha dejado de ser pertinente.

Ecuador no lo contempla, ni aun de forma indirecta, en su legislación.

Entre los elementos que configuran la pertinencia, aunque en realidad se refieren al principio de calidad, se encuentran las condiciones de cierto, veraz o correcto de la información personal: Argentina, México y Perú.

Otra de las características son las de adecuado: Argentina, Perú, República Dominicana, Panamá y Guatemala; exacto: Costa Rica, Perú y República Dominicana; completo: Costa Rica; actualizado: México, Perú y República Dominicana; y necesario: Nicaragua y Perú.

Respecto de no ser excesivo en relación al ámbito: Argentina y República Dominicana; o en relación a la finalidad, tanto de la recogida como del tratamiento: Argentina, Costa Rica, México, Perú, Panamá y República Dominicana; o respecto al propósito de recogida: Guatemala.

Si han dejado de ser pertinentes deben: destruirse, en el caso de la legislación de Argentina; cancelados, en el caso de México y Nicaragua; eliminarse o suprimirse como señala la legislación de República Dominicana o de Uruguay, aunque esta primera habla también de sustituirse si es del caso. Finalmente, el Perú determina que deben conservarse solo por el tiempo necesario para cumplir con su finalidad del tratamiento.

Del análisis realizado, la pertinencia es parte del principio de calidad de datos y no un principio *per se*, pues es condición necesaria de la primera por ser consecuente con su objetivo general. Vale la pena señalar las iniciativas respecto de la cancelación, supresión o sustitución de los datos que son incorrectos como manifestaciones del principio de calidad de datos que lo engloba.

1.5.4.3 Calidad

a) Respecto del derecho a la intimidad y a la privacidad

Desde esta perspectiva, se colige lo siguiente:

Tabla 15

País	Contenido en el principio de calidad	Contenido en otros principios
El Salvador	NO.	El artículo 32 de la Ley 534-2011 determina que los entes obligados públicos serán responsables de proteger los datos personales y, en relación con éstos, deberán: [...] c. Procurar que los datos personales sean exactos y actualizados.
Venezuela	NO.	Adecuados o proporcionales (ver pertinencia).
Bolivia	NO.	En el artículo 4 del Decreto 1793 consta como principio de veracidad, pero solo se aplica a quienes brinden servicios de certificación digital, operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación. Conforme este principio de veracidad, la información sujeta a tratamiento debe ser veraz, completa, precisa, actualizada, verificable, inteligible, prohibiéndose el tratamiento de datos incompletos o que induzcan a errores. Es decir, se recogen aquellas características que definen al principio de calidad con otro nombre.
Chile	NO.	Aunque refiriéndose al principio de finalidad de los datos, el artículo 9° de la Ley 19628 determina que los datos personales deben ser exactos, actualizados y responder con veracidad a la situación real del titular de los datos. Todos estos elementos que pueden configurar el contenido del principio de calidad de datos.
Honduras	NO.	
Paraguay	NO.	Actualización (ver pertinencia).

Fuente y elaboración: La autora (2018).

Del análisis del principio de pertinencia y de calidad realizado en la tabla 15, se concluye que Honduras no menciona en su legislación el principio de calidad y ni siquiera hace alusión a cualquiera de los elementos que lo configuran.

Venezuela y Paraguay, al referirse al principio de pertinencia, mencionan en el primer caso, que los casos deben ser proporcionales, y esta es una de las características de la pertinencia y de la calidad como principios. Asimismo, Paraguay menciona a la actualización de los datos, elemento del principio de calidad de los datos.

Únicamente, El Salvador, Bolivia y Chile mencionan los elementos que configuran el principio de calidad, esto es: exactos, actualizados, veraces, completos, precisos, verificables e inteligibles, pero tampoco lo denominan de esta manera. En el caso de Bolivia lo llaman principio de veracidad; por su parte Chile lo considera parte del principio de finalidad, y en El Salvador no es parte de un principio, sino una de las obligaciones de los entes públicos, lo que determina su aplicación limitada al ámbito público.

En suma, es necesario que los datos tengan las características de cierto, correcto, veraz, adecuado, exacto, completo, actualizado, entre otras; es decir, que se cumpla con lo que se señala en la doctrina como principio de calidad. Lamentablemente, ninguna de las legislaciones estudiadas, desde la perspectiva de la intimidad como égida de salvaguarda, ha logrado identificar este contenido esencial.

b) Respecto del derecho a la protección de datos personales

Tabla 16

País	Normativa	Cierto Correcto Veraz	Adecuado	Exacto o preciso	Completo	Actualizado	Comprobable	Comprensible o Claro	Necesario o relevante	No excesivos en relación al ámbito	No excesivos en relación a la finalidad	No excesivos para su propósito de recogida	Si han dejado de ser actualizados, completos, exactos deben destruirse
Argentina	Los numerales 1 y 7 del artículo 4, LPDP, señalan que los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido; y en el caso de que estos hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados deberán ser destruidos. Art. 4. "Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario".	SI.	SI.	SI.	SI.	SI.	NO.	NO.	NO.	SI.	Art. 4, numos. 1 y 7, LPDP. "y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido..."	NO.	SI. Art. 4. "5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley. 6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. 7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados".
Brasil	Artículo 6 de la LGPD II "(...) V - calidad de los datos: garantía a los propietarios, precisión, claridad, relevancia y actualización de los datos, de acuerdo con la necesidad y para el cumplimiento del propósito de su procesamiento (...)	NO	SI	SI	NO	SI	NO	SI	SI	NO	NO	SI	NO
Colombia	El literal d) del artículo 4º de la Ley 1581 de 2012, Ley de Protección de Datos Personales, sobre principios para el tratamiento de datos personales establece el principio de veracidad o calidad por el cual la información debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.	SI.	NO.	SI.	SI.	SI.	SI.	SI.	NO.	NO	NO.	NO.	NO.
Costa Rica	Art. 6, Ley 8968. Los datos de carácter personal solo podrá ser recolectados, almacenados o empleados para su íntegro tratamiento siempre y cuando estos	SI.	SI.	SI.	SI. El artículo 6 de la Ley 8968 señala que la	SI.	NO.	NO.	NO.	NO.	SI. Art. 6, Ley 8968. "con respecto a los	NO.	NO.

	sean: actuales, veraces, exactos y adecuados a su finalidad.				persona responsable de la base de datos tomará las medidas necesarias para que los datos sean exactos y completos.						fines para los que fueron recogidos o para los que fueron tratados posteriormente. .."		
Ecuador	NO.												
Guatemala	Decreto 57-2008, Ley de Acceso a la Información Pública. Art. 7. Actualización de información. "Los sujetos obligados deberán actualizar su información en un plazo no mayor de treinta días, después de producirse un cambio". Art. 30. Hábeas data. "Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán: [...] 4. Procurar que los datos personales sean exactos y actualizados".	NO.	NO.	SI.	NO.	SI.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
México	Art. 11, LPPDPP. El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.	SI.	NO.	NO.	NO.	SI.	NO.	NO.	NO.	NO.	Art. 11, LPPDPP. "sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados..."	NO.	Art. 11, LPPDPP. Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.
Nicaragua	NO.												
Panamá	El artículo 2, numeral 3 Ley 81 4. Principio de veracidad y exactitud: los datos de carácter personal serán exactos y puestos al día de manera que respondan con veracidad a la situación actual del propietario del dato.	SI	NO	SI	NO	SI	NO	NO	NO	NO	NO	NO	El artículo 32, numeral 5 Ley 81., El tiempo máximo que el requirente utilizará los datos y la forma como serán destruidos una vez terminado su uso.
Perú	Art. 8, Ley 29733. "Principio de Calidad: Los datos personales que vayan a ser tratados deber ser veraces, exactos y, en la medida de lo posible, actualizada, necesaria, pertinente y adecuada respecto de la finalidad para la que fueron recopilados".	SI Veraz	SI	SI	NO	SI	NO.	NO.	SI.	NO.	SI. Art. 8, Ley 29733. "respecto de la finalidad para la que fueron recopilados..."	NO.	Art. 8, Ley 29733. "Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con su finalidad del tratamiento".

República Dominicana	El artículo 5, numeral 2, de la Ley 172-13 recoge el principio de calidad de los datos, por el cual: a) Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados y pertinentes en relación al ámbito y finalidad para los que se hubieren obtenido; b) Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario".	SI.	SI.	SI.	NO.	SI.	NO.	NO.	NO.	SI.	Art. 5, núm. 2, Ley 172-13. "adecuados y pertinentes en relación al ámbito y finalidad para los que se hubieren obtenido..."	NO.	Art. 5, núm. 2, Ley 172-13. "c) Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o, en su caso, completados por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate".
Uruguay	Su contenido consta descrito en el principio de veracidad de la Ley 18.331, artículo 7, para tratar datos personales deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. En consecuencia, los datos deberán ser exactos y es de cargo de responsable actualizarlos.	SI.	SI. ecuánimes	SI.	NO.	SI.	NO.	NO.	NO.	NO.	SI. Art. 7, Ley 18.331. "no excesivos en relación con la finalidad para la cual se hubieren obtenido".	NO.	Art. 7, Ley 18.331. "de ser necesario, si ha constatado la inexactitud o falsedad de los datos, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo, deberán ser eliminados aquellos datos que hayan caducado de acuerdo a lo previsto en la presente ley".

Fuente y elaboración: La autora (2018).

Sobre el principio de calidad, se debe vincularlo directamente con el principio de pertinencia, anteriormente analizado. Esto debido a que todos los países analizados incluyen a la pertinencia en el principio de calidad: Argentina, Costa Rica, México, Perú y República Dominicana.

Por su parte, además de los países listados, Brasil, Colombia y Uruguay incluyen expresamente el principio de calidad de datos, que no tiene relación con el de pertinencia.

Esto permite concluir que si bien pueden tratarse como dos principios independientes, resulta más eficiente y claro manejar la pertinencia dentro del principio de calidad, siendo importante que su ámbito, finalidad, tratamiento y propósito sean observados para verificar su adecuación y además darle un enfoque a la seguridad y a la permanencia. Pues todos estos elementos configuran la calidad del dato.

Ahora bien, Ecuador y Nicaragua no contemplan en su legislación el principio de calidad ni aun de forma indirecta.

Entre los elementos que configuran el principio de calidad se encuentran las condiciones de cierto, veraz o correcto de la información personal: Argentina, Colombia, Costa Rica, México, Panamá, Perú, República Dominicana y Uruguay.

Otra de las características son las de adecuado: Argentina, Brasil, Costa Rica, Perú, República Dominicana y Uruguay (ecuánime); exacto: Costa Rica, Perú, República Dominicana, Guatemala, Panamá, Colombia y Uruguay; completo: Argentina, Costa Rica y Colombia; actualizado: Argentina, Brasil, México, Panamá, Perú y República Dominicana; comprobable y comprensible: Colombia; claro: Brasil; necesario: Perú y relevante: Brasil.

Respecto de no ser excesivo en relación al ámbito: Argentina y República Dominicana; o en relación a la finalidad, tanto de la recogida como del tratamiento: Argentina, Brasil Costa Rica, México, Perú, República Dominicana y Uruguay; o en cuanto al propósito de recogida: Guatemala.

Si han dejado de ser actualizados, completos, exactos deben: destruirse en el caso de la legislación de Argentina; cancelados en el caso de México y Nicaragua; eliminarse o suprimirse como señala la legislación de República Dominicana o de Uruguay, aunque esta primera habla también de sustituirse si es del caso. Finalmente, el Perú y Panamá determina que deben conservarse solo por el tiempo necesario para cumplir con su finalidad del tratamiento.

La calidad de datos como principio resulta fundamental para que los responsables tengan la obligación de precautelar sus bases de datos. Con el cumplimiento de este principio, se puede proporcionar al titular una protección preventiva que evite la interposición de recursos o acciones como la de rectificación, modificación o actualización y, en casos más graves, la de eliminación o supresión.

1.5.4.4 Finalidad

a) Respecto del derecho a la intimidad y a la privacidad

Desde esta perspectiva, se colige lo siguiente:

Tabla 17

País	Normativa	Ámbito de aplicación	Parte del principio de información
El Salvador	El artículo 32 de la Ley 534-2011 determina que los entes obligados públicos serán responsables de proteger los datos personales y, en relación con estos, deberán: [...] b. Usar los datos exclusivamente en el cumplimiento de los fines institucionales para los que fueron solicitados u obtenidos.	Ámbito público: Usar los datos para los fines institucionales para los que fueron recopilados.	
Venezuela			Como parte del derecho de información no como principio, el artículo 28 de la Constitución menciona el derecho de las personas a conocer la finalidad del registro oficial o privado de sus datos personales. En este sentido, no se ha previsto como principio que permita controlar la actuación de los responsables del fichero, sino como parte del derecho de información, es decir, del derecho a conocer para qué se utilizarán sus datos.
Bolivia	Decreto Supremo 1793. "El propósito debe ser legítimo, y previamente informadas de que sus datos serán objeto de tratamiento". Asimismo, en el artículo 56 del Decreto "Los datos personales objeto de tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro". Nuevamente, este contenido es propio del principio de finalidad; sin embargo, el "ámbito de aplicación de la ley es limitado a entidades certificadoras de firma digital".	Aplicable solo a servicios de certificación digital, operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación.	
Chile	El artículo 9° de la Ley 19628 determina que los datos personales deben utilizarse solo para los fines para los cuales hubieren sido recolectados, "salvo que provengan o se hayan recolectado de fuentes accesibles al público".		
Honduras	NO.		
Paraguay	El artículo 135 de la Constitución de la República del Paraguay establece un aspecto del principio de finalidad cuando señala que toda persona tiene derecho a conocer sobre la finalidad por la que fue recogida tratada la información personal del titular.		El artículo 8° de la Ley 1682 de 2001 señala que toda persona podrá conocer la finalidad de la recogida, uso y tratamiento de los datos personales.

Fuente y elaboración: La autora (2018).

De la tabla 17, se concluye que aquellos países que precautelan los datos desde la perspectiva limitada de la intimidad, también tienen un enfoque sectorial puesto que: El Salvador plantea el principio de finalidad aplicable solo al sector público. Bolivia únicamente lo prevé para quienes brinden servicios de certificación digital, operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación.

Venezuela y Paraguay contemplan a la finalidad no como principio, sino como condición a ser cumplida en el momento de la recogida cuando se efectiviza el deber de información, por el cual se obtiene el consentimiento previa determinación de la finalidad para la cual van a ser recolectados los datos y posteriormente tratados.

b) Respecto del derecho a la protección de datos personales

Tabla 18

País	Principio de finalidad	Deber de información	Derecho de información	Finalidad del tratamiento compatible con lo informado en su recogida	Finalidades lícitas y legítimas	Finalidades de la cesión	*Habeas data*	Bloqueo, cancelación, actualización, eliminación
Argentina	Art. 4, LPDP. "Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido".	Art. 6, LPDP. "Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios".	Art. 11, LPDP. "Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo".	Art. 3, LPDP. "3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención".	Art. 3, LPDP. "Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública".	Art.1, LPDP. "Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo."	Art. 33, LPDP. "La acción de protección de los datos personales o de hábeas data procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos".	NO.
Brasil	Art. 6 LGPD numeral I "(…) propósito: llevar a cabo el tratamiento con fines legítimos, específicos, explícitos e informados para el titular, sin la posibilidad de un tratamiento adicional incompatible con esos fines;	Art. 7 LGPD Párrafo 5. "El controlador que obtuvo el consentimiento mencionado en la sección I de la sección de este artículo que necesita comunicar o compartir datos personales con otros controladores deberá obtener el consentimiento específico del titular para este propósito, excepto en el caso de la renuncia al consentimiento previsto en esta Ley". Párrafo 7. El procesamiento posterior de los datos personales a que se refieren los párrafos 3 y 4 de este artículo puede llevarse a cabo para nuevos propósitos, siempre que los propósitos legítimos y específicos para el procesamiento posterior y	Artículo 9 LGPD El titular tiene derecho a un fácil acceso a la información sobre el procesamiento de sus datos, que debe estar disponible de manera clara, apropiada y abierta sobre, entre otras características previstas en la regulación para cumplir con el principio de libre acceso: I - propósito específico del tratamiento (…)"	Artículo 9 LGPD Párrafo 2. En caso de que se requiera el consentimiento, si hay cambios de propósito para el procesamiento de datos personales que no son compatibles con el consentimiento original, el controlador informará al titular por adelantado de los cambios de propósito, y el titular puede revocar el consentimiento si No estoy de acuerdo con los cambios	Artículo 10 LGPD § 1 Cuando el procesamiento se basa en el interés legítimo del controlador, solo se pueden procesar los datos personales estrictamente necesarios para el propósito previsto.	NO	NO	Artículo 15 LGPD La conclusión del procesamiento de datos personales se producirá en las siguientes hipótesis: I - verificación de que se ha logrado el propósito o que los datos ya no son necesarios o pertinentes para el logro del propósito específico buscado;

		la preservación de los derechos del titular, así como el fundamentos y principios establecidos en esta Ley.						
Colombia	En el artículo 4, literal b), Ley 1581 de 2012, Ley de Protección de Datos Personales se menciona entre los principios para el Tratamiento de datos personales al relativo a la finalidad, por el que el procesamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular.	Art. 12, Ley 1581 de 2012. El responsable del tratamiento, al momento de solicitar al titular la autorización deberá informarle de manera clara y expresa lo siguiente: a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;" Art. 17. Los responsables del tratamiento deberán cumplir los siguientes deberes: [...] c) Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.	NO.	NO.	Art. 4º, Ley 1581 de 2012. "b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular".	NO.	NO.	NO.
Costa Rica	Art. 6, Ley 8968. Principio de calidad de la información. "Solo podrán ser recolectados, almacenados o empleados datos de carácter personal para su tratamiento automatizado o manual, cuando tales datos sean actuales, veraces, exactos y adecuados al fin para el que fueron recolectados".	NO.	Art. 7, Ley 8968. Derechos que le asisten a la persona. 1.- Acceso a la información. "[...] b) Recibir la información relativa a su persona, así como la finalidad con que fueron recopilados y el uso que se le ha dado a sus datos personales. El informe deberá ser completo, claro y exento de codificaciones. Deberá estar acompañado de una explicación de los términos técnicos que se utilicen".	Art. 6, Ley 8968. Principio de calidad de la información. "4.- No se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando se establezcan las garantías oportunas para salvaguardar los derechos contemplados en esta ley".	Art. 6, Ley 8968. Principio de calidad de la información. "4.- Adecuación al fin. Los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. Las bases de datos no pueden tener finalidades contrarias a las leyes ni a la moral pública".	NO.	NO.	Art. 6, Ley 8968. "1.- Actualidad. Los datos de carácter personal deberán ser actuales. El responsable de la base de datos eliminará los datos que hayan dejado de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos y registrados".

Ecuador	SI.	NO.	Art. 92, Constitución de la República del Ecuador. "Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos".	NO.	NO	NO.	NO.	NO.
Guatemala	SI.	El artículo 30, numeral 3, Decreto 57-2008, LAIP, hace mención a la obligación del sujeto de poner a disposición de la persona individual, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento.	NO.	NO.	NO.	NO.	Art. 9, núm. 4. "Habeas data: Es la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización".	NO.
México	Art. 6, LPDPP. "Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley". Art. 11. "El responsable procurará que los datos	Art. 16, LPDPP. "El aviso de privacidad deberá contener, al menos, la siguiente información: [...] II. Las finalidades del tratamiento de datos".	NO.	Art. 12, LPDPP. "El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en el aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular".	Art. 9, LPDPP. "Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca. No podrán crearse bases de datos que contengan datos personales	Art. 13, LPDPP. "El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad". Art. 36. "Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el	NO.	Art. 3, III. LPDPP. Bloqueo. "La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos

	personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados".				sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado".	aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento".		que corresponde". Art. 11. LPDPP. "Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados".
Nicaragua	Art. 7, lit. a) y Art. 9, Ley 787. La finalidad como principio se visibiliza en la recogida de la información, en el tratamiento de los datos, en su cesión y en su vigencia temporal en un fichero.	Art. 7, Ley 787. Obligación de informar al obtener los datos personales. "El responsable de los ficheros de datos personales deberá informar previamente a los titulares de los mismos de forma expresa y clara lo siguiente: a) La finalidad para la que serán utilizados y quiénes pueden ser sus destinatarios o clase de destinatarios".	Art. 16, Ley 787. Derecho a solicitar información. "El titular de los datos puede solicitar información a la Dirección de Protección de Datos Personales, relativa a la existencia de ficheros de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita".	NO.	Art. 9, Ley 787. Sobre el tratamiento de datos personales. "Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas en la presente Ley. Los datos personales sólo podrán ser tratados, cuando sean adecuados, proporcionales y necesarios en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan solicitado".	Art. 15, Ley 787. Procedimiento para la cesión y transferencia de datos. "Para la cesión y transferencia de datos personales y que se encuentren en ficheros de datos públicos o privados, se deberá cumplir el siguiente procedimiento: a) La cesión y transferencia de datos personales se realizará a solicitud de una persona legalmente autorizada; b) La solicitud deberá contener el objeto y la finalidad que se persigue con dicha información".	Art. 19, Ley 787. Derechos de modificación de los datos. "Toda persona tiene derecho a: a) [...] Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad que dio lugar a su tratamiento. [...] f) A que los datos personales se conserven durante cinco años o por el término que las disposiciones contractuales entre las partes acuerden, así como cuando éstos hayan dejado de ser adecuados, proporcionales y necesarios para el ámbito y las finalidades que fueron solicitados".	Art. 3, Ley 787. Definiciones. Para la presente ley se entiende por: " b) Bloqueo: Es la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en el fichero de datos en el que se encuentran".
Panamá	Art. 42, Constitución de Panamá. La información personal solo podrá ser recogida para fines específicos, mediante consentimiento de su	Art. 4, numeral 17 de la Ley 81: "Responsable del tratamiento de los datos. Persona natural o jurídica, de derecho público o privado, lucrativa o no, que le corresponde las	SI Artículo 15. Ley 81 (…) 1. Derecho de acceso: permite al titular obtener sus datos personales que encuentren almacenados o sujetos a tratamiento en	SI artículo 2 numeral 2 de la Ley 81. 2. Principio de finalidad: los datos personales deben ser recolectados con fines determinados y no ser tratados posteriormente para	NO.	NO.	NO.	SI, artículo 2 numeral 2 de la Ley 81 "(…) ni conservar por tiempo mayor del necesario para los fines de tratamiento

	titular o por disposición de autoridad competente con fundamento en lo previsto en la ley. El artículo 2 numeral 2 de la Ley 81 estipula que el principio de finalidad es aquel por el cual los datos personales "deben ser recolectados con fines determinados y no ser tratados posteriormente para fines incompatibles o distintos para los que se solicitaron".	decisiones relacionadas con el tratamiento de los datos y que determina los fines, medios y alcance, así como cuestiones relacionadas a estos.	bases de datos de instituciones públicas o privadas, además de conocer el origen y la finalidad para los cuales han sido recabados.	fines incompatibles o distintos para los se solicitaron.				
Perú	El artículo 6 de la Ley de Protección de Datos Personales señala que el principio de finalidad establece que los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita.	Art. 6, LPDP. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.	NO.	NO.	El artículo 6 de la Ley de Protección de Datos Personales señala que el principio de finalidad establece que los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita.	NO.	NO.	NO.
República Dominicana	El artículo 5 numeral 8 de la Ley 172-13 recoge el principio de finalidad de los datos, mediante el cual se faculta recoger datos personales para su tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para los que se hayan obtenido.	Art. 5, núm. 8, Ley 172-13. "El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando el principio de calidad, es decir: a) Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados y pertinentes en relación al ámbito y finalidad para los que se hubieren obtenido".	Art. 5, Ley 172-13. Derecho de información. "Cuando se recaben datos personales que requieran del consentimiento del titular de los datos, para que se les pueda dar el tratamiento de datos o ser cedidos después de obtener dicho consentimiento, se deberá informar previamente, a por lo menos uno de los titulares de los datos, en forma expresa y clara, explicando: a) La finalidad para la que serán destinados y quiénes pueden ser sus destinatarios o clase de destinatarios".	NO.	Art. 5, núm. 8, Ley 172-13. Finalidad de los datos. "Los datos solo se recogerán para su tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para los que se hayan obtenido".	NO.	NO.	NO.

Uruguay	Art. 8, Ley 18.331. “los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención y deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados”.	Art. 7º, Ley 18.331. Principio de veracidad. “Los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley”.	Art. 13, Ley 18.331. Derecho de información frente a la recolección de datos. “Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios”.	Art. 8º, Ley 18.331. Principio de finalidad. “Los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención”.	Art. 6º, Ley 18.331. Principio de legalidad. “La formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia. Las bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública”.	Art. 17, Ley 18.331. “Los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo”. Art. 8, Ley 18.331. “[...] y por ello tampoco podrán comunicarse datos entre bases de datos, sin que medie ley o previo consentimiento informado del titular pues es necesario que el titular conozca las nuevas finalidades a las que se pretende someter los datos”.	Art. 37. Habeas data. Ley 18.331. “Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicas o privadas; y -en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización- a exigir su rectificación, inclusión, supresión o lo que entienda corresponder”.	Art. 8, Ley 18.331. “[L]os datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención y deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados”.

Fuente y elaboración: La autora (2018).

Argentina, Colombia, Costa Rica, Ecuador, Guatemala, México, Nicaragua, Panamá, Perú, República Dominicana, Panamá y Uruguay reconocen a nivel constitucional y legal el principio de finalidad. Este es uno de los pocos que pese a lo variado de su alcance ha sido parte de todas las normativas analizadas. Es, entonces, un principio fundamental para el desarrollo del derecho a la protección de datos personales.

Resta identificar los niveles de acción que pueden abarcar la finalidad. Si bien Costa Rica incluye el principio de finalidad en el de calidad, esto no motiva que exista una variante en su conceptualización, toda vez que solo podrán almacenarse datos personales que correspondan a la finalidad para la que fueron recabados.

En Argentina, Brasil, Colombia, Guatemala, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay consta expresamente como parte del deber de información, que los responsables del tratamiento informen sobre la finalidad de la recolección, uso, tratamiento y cesión de los datos personales.

Asimismo, Argentina, Brasil, Nicaragua, República Dominicana, Costa Rica y Ecuador conciben, desde la perspectiva del derecho de información, que los titulares tengan la prerrogativa de exigir al responsable del tratamiento el acceso y conocimiento de la finalidad de la recolección, uso, tratamiento y cesión de los datos personales. Panamá lo incluye en el derecho de acceso.

Es obligatorio, entonces, que la finalidad del tratamiento sea compatible con lo informado en su recogida conforme lo señalan legislaciones como la argentina, brasileña, mexicana, panameña, costarricense y uruguaya, en las cuales si esta compatibilidad no existe, se debe solicitar nuevamente consentimientos al titular, se activan obligaciones de eliminación por parte de los responsables del tratamiento o la exigibilidad de los derechos de los titulares.

Varios países determinan que las finalidades siempre deben ser lícitas y legítimas en salvaguarda de los titulares del dato personal: Argentina, Colombia, México, Uruguay y Costa Rica.

Acápite especial merece el tema de informar al titular sobre las finalidades de la cesión de sus datos a otros responsables, como es el caso de Argentina, México, Nicaragua y Uruguay.

Acerca del *habeas data*, como acción, se determina el derecho de los titulares de exigir conocer la finalidad y uso de sus datos, así como verificar situaciones anómalas que faculten el acceso, rectificación o eliminación de los datos personales; este es el caso de Argentina, Nicaragua, Guatemala (únicamente bases de datos de responsables públicos) y Uruguay.

Brasil y Panamá establecen la obligación de eliminar los datos una vez que se han agotado los propósitos de la recogida.

Finalmente, se establece el bloqueo, por el cual se permite la identificación y conservación de los datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de estas, tal como

señala México y Nicaragua. Por su parte, se determina la actualización, cancelación o eliminación cuando la finalidad para la cual se recabó el dato se encuentra cumplida, conforme señala México, Costa Rica y Uruguay.

Luego del análisis realizado, se puede concluir que el país que legisla de mejor manera el principio de finalidad es Uruguay, debido a que visualiza este principio como un deber del obligado, un derecho del titular; determina la necesidad de que la finalidad del tratamiento sea compatible con lo informado en su recogida; que estas además sean lícitas y legítimas; que exista identificación de las finalidades en la cesión de datos, el derecho a conocer la finalidad y uso de los datos, desde la perspectiva de acciones como el *habeas data*, así como el bloqueo, la actualización, la cancelación y la eliminación por haberse agotado la finalidad para la cual fue recabado el dato o suscitarse incompatibilidades.

Desde las directrices para la regulación de los archivos de datos personales informatizados, Resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990,[1535] existen dos enfoques relativos a la finalidad que debieran tomarse en cuenta en el momento de la incorporación en las legislaciones de cada país; estas son: la imposibilidad de levantar la confidencialidad para fines incompatibles y sin autorización del titular y la mención sobre la temporalidad de la permanencia de los datos en relación con sus fines.

1.5.4.5 Seguridad

a) Respecto del derecho a la intimidad y a la privacidad

Desde esta perspectiva, se colige lo siguiente:

Tabla 19

País	Normativa	Medidas de seguridad	Objetivo	Ámbito de aplicación
El Salvador	Art 32, Ley 534-2011. "los entes obligados públicos serán responsables de proteger los datos personales y, en relación con éstos, deberán: e. Adoptar medidas que protejan la seguridad de los datos personales".	SI.	Art 32, Ley 534-2011. "[...] Evitar alteración, pérdida, transmisión y acceso no autorizado".	Público.
Venezuela	SI. En la Ley Infogobierno de 2013 existe la mención a la necesidad de salvaguarda la seguridad de los datos que estén bajo la responsabilidad de entes estatales".		SI. Art. 54, Ley Infogobierno de 2013. "a fin de resguardar la autenticidad, integridad, inviolabilidad y confiabilidad de los datos, información y documentos electrónicos..."	Público. Arts. 54 y 55, Ley Infogobierno. La Superintendencia de Servicios de Certificación Electrónica se considera órgano competente en materia de seguridad informática y es responsable del desarrollo, implementación, ejecución y seguimiento al Sistema Nacional de Seguridad Informática, de implementar entre el Poder Público y en el Poder Popular las iniciativas de seguridad informática, dirigidas a la privacidad, protección de

[1535] Asamblea General de Naciones Unidas, "Res 45/95 Principios rectores para la reglamentación de los ficheros automatizados de datos personales", *Documentos oficiales de las Naciones Unidas*, 1989, accedido 20 de julio de 2017, http://www.un.org/es/comun/docs/?symbol=%20A/RES/45/95&Lang=S.

				datos y de infraestructuras críticas, así como intervenir y dar respuesta ante los riesgos y amenazas que atenten contra la información que manejen.
Bolivia		Art. 4, Decreto Supremo 1793. "entre los principios aplicables a las entidades certificadoras que traten datos personales, el de seguridad por el cual, en el tratamiento deberán implementar controles técnicos, administrativos que se requieran".	El Decreto Supremo 1793, en el artículo 4, habla sobre preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento.	Aplicables a las entidades certificadoras que traten datos personales
Chile	NO.			
Honduras	NO.			
Paraguay	NO.			

Fuente y elaboración: La autora (2018).

Según se desprende de la tabla 19, Chile, Honduras y Paraguay no mencionan siquiera el principio de seguridad como forma de precautelar datos personales. En los restantes países, esto es Bolivia, Venezuela y El Salvador, se menciona la necesidad de seguridad pero no se hace alusión alguna a mecanismos aplicables o mayor detalle que la obligación general de implementar medidas de seguridad o controles administrativos y técnicos o estándares técnicos y operativos.

Únicamente, El Salvador y Venezuela tienen normativas de carácter sectorial pues solo se aplican al sector público. En el caso de Bolivia, rige exclusivamente a entidades certificadoras de firmas que tratan datos personales. Es decir, estas medidas de seguridad que son criterio básico del manejo responsable de datos personales no son de aplicación general.

Finalmente, el objetivo de la implementación de estas medidas de seguridad son las de velar por evitar alteración, pérdida, transmisión, falsificación, extravío, utilización y acceso no autorizado o fraudulento, a fin de resguardar la autenticidad, preservar la confidencialidad, disponibilidad, autenticidad, no repudio integridad, inviolabilidad y confiabilidad de los datos, información y documentos electrónicos, brindando seguridad a los registros, conforme señalan Bolivia, Venezuela y El Salvador.

b) Respecto del derecho a la protección de datos personales:

Tabla 20

País	Normativa	Medidas técnicas	Medidas administrativas u organizativas	Medidas humanas o físicas o lógicas	Medidas legales	Objetivo	Evitar	Prohibiciones
Argentina	Núm. 1, art. 9, LPDP. "[E]l responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado".	SI.	SI.	NO.	NO.	Art. 9, núm. 1, LPDP. "[G]garantizar la seguridad y confidencialidad de los datos personales..."	Art. 9, núm. 1, LPDP. "Adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado..."	Art. 9, núm. 2, LPDP. "prohibición de registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad..."
Brasil	Art. 6 numeral VII LGPD "(...) "utilización de medidas técnicas y administrativas capaces de proteger los datos personales de accesos no autorizados y de situaciones accidentales o ilícitas de destrucción, pérdida, alteración, comunicación o difusión".	SI	SI	NO	NO	Art. 6 LGPD "(...) proteger los datos personales del acceso no autorizado y la destrucción, pérdida, alteración, comunicación o difusión accidental o ilegal	Art. 6 LGPD "(...) de accesos no autorizados y de situaciones accidentales o ilícitas de destrucción, pérdida, alteración, comunicación o difusión".	Artículo 44. El procesamiento de datos personales será irregular cuando no cumpla con la ley o cuando no brinde la seguridad que el titular puede esperar,
Colombia	Según el literal g) del artículo 4º de la Ley 1581, "se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de datos personales..."	SI.	SI.	SI. Humanas.		Art. 4º, lit. g), Ley 1581. "Seguridad de los registros".	Art. 4º, lit. g), Ley 1581. "adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de datos personales..."	
Costa Rica	Según el artículo 10 de la Ley 8968, "el responsable de la base de datos deberá adoptar las medidas necesarias para garantizar la seguridad de los datos de carácter personal y la protección de la información almacenada frente a acciones contrarias a la ley, estableciendo mecanismos de seguridad física y lógica de acuerdo con el desarrollo tecnológico actual..."	NO.	NO.	SI. Art. 10, Ley 8968. "Físicas y lógicas de acuerdo al desarrollo tecnológico actual..."	NO.	Art. 10, Ley 8968, "garantizar la seguridad de los datos de carácter personal y la protección de la información almacenada..."	Art. 10, Ley 8968. "(...) frente a acciones contrarias a la ley..."	Art. 10, Ley 8968. "no se registrarán datos personales en bases de datos que no reúnan todos los requisitos para garantizar su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas..."
Ecuador	Art. 92, Constitución de la República del Ecuador de 2008. Limitado para el caso de datos sensibles.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Guatemala	El numeral 5 del artículo 30 del Decreto 57-2008 "señala la responsabilidad de los sujetos obligados de implementar las medidas necesarias que garanticen la seguridad, y en su caso confidencia o reserva de los datos personales y eviten su alteración, pérdida, transmisión y acceso no	NO.	NO.	NO.	NO.	Art. 30, núm. 5, Decreto 57-2008. "Medidas para guardar reserva y confidencialidad de los datos personales..."	Art. 30, núm. 5., Decreto 57-2008. "Alteración, pérdida, transmisión y acceso no autorizado..."	NO.

	autorizado…"							
México	Según el artículo 19, LPDPP, "todo responsable deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado…"	SI.	SI.	SI.	NO.	Art. 19, LPDPP. "proteger los datos personales…"	Art. 19, LPDPP. "Contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado…"	NO.
Nicaragua	Arts. 9 y 11 de la Ley de Protección de Datos. Art. 3, Reglamento de la Ley 787. Ley de Protección de Datos Personales, Decreto 36-2012. Al referirse a las definiciones sobre medidas de seguridad establece tres clases: Las medidas de seguridad físicas, las medidas de seguridad organizativas y las medidas de seguridad técnicas. El responsable del fichero deberá adoptar las medidas de índole técnicas y organizativas necesarias para garantizar la integridad, confidencialidad y seguridad de los datos".	SI.	SI.	SI.	NO.	Arts. 9 y 11, Ley de Protección de Datos. "garantizar la integridad, confidencialidad y seguridad de los datos…"	Arts. 9 y 11, Ley de Protección de Datos. "evitar su acceso, uso, alteración, pérdida, revelación, transferencia, tratamiento, consulta, revelación o divulgación no autorizada, y que permitan detectar desviaciones, intencionales o no, de información privada, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado…"	NO.
Panamá	El artículo 2 de la Ley 81, el principio de seguridad de los datos dispone que los responsables del tratamiento de los datos personales deban: (…) adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los bajo su custodia, principalmente cuando se trate de datos considerados sensibles, e informar al titular, lo más pronto posible, cuando los datos hayan sido sustraídos sin autorización o haya indicios suficientes de que seguridad ha sido vulnerada.	SI.	SI.	SI.	NO.	Artículo 2 de la Ley 81, "(…) garantiza la seguridad de los datos bajo su custodia, principalmente cuando se trate de datos considerados sensibles."	El artículo 9 de la Ley 81, "(…) garantizar que los datos hayan sido sustraídos sin autorización o haya indicios suficientes de que su seguridad ha sido vulnerada.	NO.
Perú	Según el artículo 9 de la Ley de Protección de Datos Personales "el principio de seguridad como aquel por el cual el titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales…"	SI.	SI.	NO.	SI.	Art. 9, Ley de Protección de Datos Personales. "garantizar la seguridad de los datos personales…"	NO.	NO.
República Dominicana	El artículo 5, numeral 5, de la Ley 172-13 señala que "el principio de seguridad de los datos establece que el responsable del archivo de datos personales y en su caso, el encargado del tratamiento, deberán adoptar e implementar las medidas de índole técnica, organizativa y de seguridad necesarias para salvaguardar los datos de carácter personal y eviten su alteración, pérdida, tratamiento, consulta o acceso no autorizado".	SI.	SI.	NO.	NO.	Art. 5, núm. 5, Ley 172-13. "salvaguardar los datos de carácter personal…"	Art. 5, núm. 5, Ley 172-13. "eviten su alteración, pérdida, tratamiento, consulta o acceso no autorizado. Art. 5, núm. 5, Ley 172-13. "c) Las Sociedades de Información Crediticia (SIC) deben adoptar medidas apropiadas para proteger sus bases de datos contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informáticos…"	Art. 5, núm. 5, Ley 172-13. "En consecuencia: a) Queda prohibido registrar datos personales en archivos, registros o bancos de datos que no reúnan condiciones técnicas de integridad y seguridad…"
Uruguay	Art. 10, Ley 18.331. "[E]l responsable o usuario de la base de datos deberá adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Estas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Queda prohibido registrar datos personales en bases de datos que	SI.	SI.	NO.	NO.	Art. 10, Ley 18.331. "garantizar la seguridad y confidencialidad de los datos personales…"	Art. 10, Ley 18.331. "Estas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado…"	Art. 10, Ley 18.331. "Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad…"

no reúnan condiciones técnicas de integridad y seguridad".

Art. 7º, Decreto 414/009. "[D]deben cumplir con las medidas de seguridad cuando señala que tanto el responsable como el encargado de la base de datos o tratamiento deberán proteger los datos personales que sometan a tratamiento…"

El artículo 7º del Decreto 414/009 establece como concepto de seguridad como aquellas medidas técnicas y organizativas que resulten idóneas para garantizar su integridad, confidencialidad y disponibilidad de los datos personales.

Fuente y elaboración: La autora (2018).

Desde la perspectiva de la protección de los datos personales como derechos casi todos los países, en ámbito público y privado contemplan el principio de seguridad, excepto Ecuador que solo lo contempla a nivel constitucional y para datos sensibles.

Aquellos países que consideran que la seguridad incluye el diseño y la implementación de medidas técnicas, administrativas u organizativas son: Argentina, Brasil, Colombia, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay. Anotándose que, Colombia hace mención a medidas humanas, como aquellas brechas de seguridad provocadas por acciones de personas. Asimismo, México, Nicaragua y Costa Rica, hablan de medidas físicas, que pueden entenderse desde la infraestructura hasta la materialidad de los espacios en los cuales se recaba o tratan datos. Finalmente, Costa Rica habla de medios lógicos y Perú de medios legales; estas innovaciones pudieran ser interesantes para identificar que las medidas de seguridad también deben ser previstas en estas esferas de aplicación.

Excepto Ecuador, como regla general el objetivo de las medidas de seguridad son garantizar, salvaguardar, proteger los datos personales; ya no existen equívocos como los que se analizó en la tabla 20 en la cual se habla de integridad, no repudio y otros objetivos distintos a la naturaleza propia del dato.

Con estos mecanismos se pretenden evitar su acceso, uso, adulteración, alteración, pérdida, sustracción, revelación, comunicación, transferencia, tratamiento, consulta, o tratamiento no autorizado o fraudulento, y que permitan detectar desviaciones, intencionales o no, de información, tal como señalan los países analizados menos Perú. Panamá menciona además, indicios suficientes de que la seguridad ha sido vulnerada, esto porque establece la obligación de la notificación sobre vulneraciones al titular y a la entidad reguladora.

República Dominicana desarrolla una obligación específica para las Sociedades de Información Crediticia (SIC), esto es la de adoptar medidas apropiadas para proteger sus bases de datos contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informáticos. Esta expresa mención podría criticarse por que pudiera considerarse taxativa y no ejemplificativa, puesto que en las medidas físicas, técnicas y administrativas se encuentran incluidas.

Finamente, Argentina, Costa Rica, República Dominicana y Uruguay establecen la prohibición de registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad. Brasil señala que se entenderá como procesamiento irregular cuando o ilegal cuando no se brinde la seguridad que el titular puede esperar,

En conclusión, el principio de seguridad en la protección de datos personales es vital, prueba de ello es que consta de manera homogénea en las legislaciones estudiadas, incluso en aquellas basadas en la protección limitada a la intimidad. Sin embargo, siguen siendo normativas de segunda generación que deberán adaptarse a los nuevos estándares de protección previstos en el reglamento europeo de protección de datos personales.

1.5.4.6 Consentimiento

a) Respecto del derecho a la intimidad y a la privacidad

Desde esta perspectiva, se colige lo siguiente:

Tabla 21

País	Norma	Consentimiento	Expreso	Libre	Escrito	Medio equivalente	Del titular	Previo	Informado	Revocable
El Salvador	El artículo 33 de la Ley 534-2011 señala que los entes obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información administrados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso y libre, por escrito o por un medio equivalente, de los individuos a que haga referencia la información.	SI.	SI.	SI.	SI.	SI.	SI.	NO.	NO.	NO.
Venezuela	NO.									
Bolivia	En el Decreto Supremo 1793, artículo 3, IV, literal b), consta que el consentimiento será previo, expreso e informado del titular, por escrito u otro medio equiparable de acuerdo con las circunstancias; incluso podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo.	SI.	SI.	NO.	SI.	SI. Medio equiparable de acuerdo con las circunstancias.	SI.	SI.	SI.	SI. Art. 56. Revocable cuando exista causa justificada, pero no tendrá efecto retroactivo.
Chile	Art. 4, Ley 19628. La persona titular del dato debe autorizar, por escrito, su tratamiento para los propósitos para los que se solicitó su almacenamiento y su posible comunicación al público. Podrá ser revocada, aunque sin efecto retroactivo; lo que también deberá hacerse por escrito.	Autorizar.	SI Art. 17, Ley 19628. En los casos de relativos a obligaciones de carácter económico, financiero, bancario o	NO.	SI.	NO.	SI.	NO.	NO.	SI.

			comercial.						
			Art. 24, Ley 19628. Las recetas médicas y exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados.						
Honduras	NO.								
Jamaica	En el artículo 19 de la Constitución de Jamaica consta como piedra angular el consentimiento, ya que solo este autoriza a la búsqueda de una persona o de su propiedad o a la entrada de otros en sus instalaciones.	Consentimiento para la búsqueda de la persona o su propiedad o la entrada en sus instalaciones.							
Paraguay	Normativa sectorial que se limita a regular los datos personales contenidos en ficheros oficiales o ficheros privados de carácter público, incluidos los de solvencia económica y situación patrimonial, es decir ficheros autorizados y regulados por la ley por considerarlos de interés general. En el artículo 5 señala que podrán ser publicados o difundidos solamente cuando sus titulares hubiesen otorgado autorización expresa y por escrito para el efecto.	Autorización.	SI.	NO.	SI.	NO.	NO.	NO.	NO.

Fuente y elaboración: La autora (2018).

El consentimiento es el principio más importante de aquellos que protegen los datos personales independientemente de que se los proteja basados en la intimidad; sin embargo, como se registra en la tabla 21, ni Venezuela ni Honduras los contemplan en su normativa. Jamaica, por su parte, tiene una forma especial de recogerlo porque al hacer alusión a él se refiere a búsqueda de la persona o su propiedad o la entrada en sus instalaciones. Por su parte, El Salvador, Bolivia, Chile, Paraguay y Brasil coinciden con su debido reconocimiento.

Las diferencias radican en sus condiciones básicas; es decir, si el consentimiento debe ser expreso (El Salvador, Bolivia, Chile, Paraguay y Brasil), libre (El Salvador y Brasil), escrito (El Salvador, Bolivia, Chile, Paraguay, excepto Brasil), o a través de otro medio equivalente o equiparable (El Salvador y Bolivia), por parte de su titular (El Salvador, Bolivia, Chile y Brasil que lo considera usuario, menos Paraguay), previo (únicamente Bolivia); informado (Bolivia y Brasil), puede ser revocable pero no tendrá efecto retroactivo (Bolivia y Chile).

En el caso de Bolivia, si bien el consentimiento es previo e informado por parte del titular, por escrito y revocable cuando exista causa justificada, sin embargo, su aplicación es limitada; es decir, para llevar a cabo el tratamiento de datos personales por una entidad certificadora autorizada (arts. 3, IV, b, 56 y 39, Decreto 1793). Lo mismo ocurre en el caso de Brasil, que también es de aplicación limitada a los servicios de internet y telecomunicaciones, y por eso este principio se lo reconoce al usuario.

b) Respecto del derecho a la protección de datos personales:

Tabla 22

País	Consentimiento	Expreso	Tácita	Específica	Inequívoco	Libre	Escrito	Medio equivalente	Del titular	Previo	Informado	Cesión	Revocable
Argentina	SI. Art. 5, LPDP. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo con las circunstancias. Junto con otras declaraciones, deberá figurar en forma expresa y destacada.	SI. Expresa y destacada.	NO.	NO.	NO.	SI.	SI.	SI. O por otro medio que permita se le equipare, de acuerdo con las circunstancias.	SI.	NO.	SI.	Art. 11, LPDP. "(Cesión). 1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo..."	SI. Art. 11, LPDP. "(Cesión). 2. El consentimiento para la cesión es revocable".
Brasil	El artículo 5, acápite XII, de la Ley LGPD señala que "el	NO	NO	SI, Art. 5 acápite XII LGPD consentimien	SI	SI	SI, Artículo 8 El consentimiento previsto en el	NO	SI	NO	SI	Art. 7 Párrafo 5 LGPD "El controlador que obtuvo el	SI, Puede ser revocado en cualquier momento, por

	consentimiento es la manifestación libre, informada e inequívoca por la cual el titular acuerda el tratamiento de sus datos personales para una finalidad determinada;”.			to para una finalidad determinada Párrafo 4. El consentimiento será para fines específicos, y las autorizaciones genéricas para el procesamiento de datos personales serán nulas.			artículo I del art. 7 de esta Ley se proporcionará por escrito o por otros medios que demuestren la manifestación de voluntad del titular.				consentimiento mencionado en la sección I de la sección de este artículo que necesita comunicar o compartir datos personales con otros controladores deberá obtener el consentimiento específico del titular para este propósito, excepto en el caso de la renuncia al consentimiento previsto en esta Ley.”	manifestación expresa del titular, sobre todo si han existido modificaciones a las condiciones iniciales con las que este fue emitido, artículo 8 y 9 de la LGPD
Colombia	SI. Autorización. Art. 3°, Ley 1581 de 2012. Definiciones. “Para los efectos de la presente ley, se entiende por: a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales...” Art. 9°. Ley 1581 de 2012. “Autorización del Titular. Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior”.	SI.	NO.	NO.	NO.	NO.	NO.	SI. Art. 9°, Ley 1581 de 2012. “por cualquier medio que pueda ser objeto de consulta posterior...”	SI.	SI.	SI.	SI. Lit. c), art. 4º, Ley 1581 de 2012. “Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento...”	NO.
Costa Rica	SI. Art. 5, Ley No. 8968. “2.- Otorgamiento del	SI.	NO.	NO. Preciso.	SI.	NO.	SI.	SI. Físico o	SI. Del titular o su	SI. Art. 5, Ley 8968. Principio de	SI. Art. 5, Ley 8968.	SI. Art. 7, Ley 8968. “Derechos que le	SI. Art. 5, Ley 8968. “Este

	consentimiento.- Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante".						electrónico.	representante.	consentimiento informado. 1.- Obligación de informar. "Cuando se soliciten datos de carácter personal será necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco".	Principio de consentimiento o informado. 1. Obligación de informar. "Cuando se soliciten datos de carácter personal será necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco..."	asisten a la persona. Se garantiza el derecho de toda persona al acceso de sus datos personales, rectificación o supresión de estos y a consentir la cesión de sus datos..."	consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo".
Ecuador	SI. Art. 66, Constitución de la República del Ecuador. Se reconoce y garantizará" a las personas: [...] 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley".	Art. 9, LCEFEMD. Protección de datos. "Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente de l uso o transmisión de mensajes de datos".	NO.	NO.	NO.	NO.	NO.	NO.	SI.	NO.	NO.	SI. Art. 9, LCEFEMD. "se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. [...] los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente".	SI. Art. 9, LCEFEMD. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.
Guatemala	SI. Art. 31, Decreto 57-2008. Consentimiento expreso. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos	SI.	NO.	NO.	NO.	NO.	SI.	NO.	SI. Art. 31, Decreto 57-2008. Consentimiento expreso. Los sujetos obligados no podrán	NO.	NO.	NO.	NO.

	personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones, salvo que hubiere mediado el consentimiento expreso por escrito de los individuos a que hiciere referencia la información. El Estado vigilará que en caso de que se otorgue el consentimiento expreso, no se incurra en ningún momento en vicio de la voluntad en perjuicio del gobernado, explicándole claramente las consecuencias de sus actos.								difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones, salvo que hubiere mediado el consentimiento expreso por escrito de los individuos a que hiciere referencia la información.				
México	SI. Art. 3. LPDPSO. "Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos [...] Dicho consentimiento debe ser expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición".	SI. Art. 21, LPDPSO. El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología. Art. 8, LPDPP. Los datos financieros o patrimoniales requerirán el	SI. Art. 21, LPDPSO. El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, este no manifieste su voluntad en sentido contrario. Por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se	SI. Art. 20, LPDPSO. "II. Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento".	NO.	SI. Art. 20, LPDPSO. "I. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular..."	NO. Art. 21, LPDPSO. Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de esta ley.	SI. Art. 8, LPDPP. El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.	SI. Art. 3, LPDPSO. Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos.	SI. Art. 20, LPDPSO. "Cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la presente Ley, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales".	SI. Art. 20, LPDPSO. "III. Informada: Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales. En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, se estará a lo dispuesto en las reglas de representación previstas en la	SI. Art. 27, LPDPSO. "III. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar: a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y b) Las finalidades de estas transferencias; IV. Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de	SI. Art. 8, LPDPP. El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos. Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.

		consentimiento expreso de su titular, salvo las excepciones a que se refieren los artículos 10 y 37 de la presente ley.	manifieste expresamente. Art. 8, LPDPP. Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.								legislación civil que resulte aplicable".	datos personales que requieren el consentimiento del titular..."	
Nicaragua	SI. Manifestación voluntaria. Art. 3, Ley de Protección de Datos. "d. Consentimiento del titular: Es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular de los datos consiente el tratamiento de sus datos personales". "Las normas de la presente Ley no se aplicarán a las encuestas de opinión; investigaciones científicas o médicas, y a las actividades análogas".	NO.	NO.	SI.	SI	SI. Libre.	SI. Art. 6. Consentimiento. "El consentimiento deberá ser otorgado por escrito o por otro medio idóneo, físico o electrónico".	SI. Art. 6. Consentimiento. "El consentimiento deberá ser otorgado por escrito o por otro medio idóneo, físico o electrónico".	SI. Art. 6. Consentimiento. "El titular de los datos deberá dar por sí o por su representante legal o apoderado el consentimiento para la entrega de los datos, salvo que la ley disponga otra cosa dentro de los límites razonables. La razonabilidad deberá ser considerada por la Dirección de Protección de Datos Personales, si se le planteare alguna controversia. Lo anterior tiene tanto para los	NO.	SI.	SI. Art. 13. Cesión y transferencia de datos personales. "Los datos personales se podrán ceder y transferir cuando, los fines estén directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le deberá informar sobre la finalidad de la cesión e identificar al cesionario". Art. 27. Datos relativos a las	SI. Art. 6. "Dicho consentimiento podrá ser revocado sin efecto retroactivo, por cualquiera de los medios permitidos por la ley..." Art. 13. "El consentimiento para la cesión es revocable, mediante notificación por escrito o por cualquier otra vía que se le equipare, según las circunstancias, al responsable del

									ficheros de datos de titularidad pública como privada".			encuestas pueden cederse previo consentimiento del titular.	fichero de datos".
Panamá	SI. Art. 42, Constitución panameña. "Esta información sólo podrá ser recogida para fines específicos, mediante consentimiento de su titular o por disposición de autoridad competente con fundamento en lo previsto en la Ley". Artículo 2 numeral 8 de la Ley 81 establece que para que exista licitud en el tratamiento de un dato personal este deberá ser "recolectado y tratado con el consentimiento previo, informado e inequívoco del titular del dato o por fundamento legal.". El numeral 4 del artículo 4 de la Ley 81, al definir consentimiento señala que es "la manifestación de la voluntad del titular de los datos, mediante la cual se efectúa el tratamiento de estos.	NO.	NO.	SI.	SI	NO.	NO.	NO.	SI., Art. 6 Ley 81, determina que el consentimiento debe mantener su "trazabilidad mediante documentación, ya sea electrónica o mediante cualquier otro mecanismo que resulte adecuado al medio de que se trate el caso".	SI	SI	SI... Art. Artículos 25. Los responsables del tratamiento de datos solo podrán transferir información sobre estos cuando cuenten con el consentimiento previo, informado e inequívoco del titular, **salvo las excepciones establecidas en esta Ley o en las leyes especiales.**	SI, Art... 6, numeral 4 de la Ley 81, determina que "(…) El consentimiento podrá obtenerse de forma que permita su trazabilidad mediante documentación, ya se electrónica o mediante cualquier otro mecanismo que resulte adecuado al medio de que se trate el caso y podrá ser revocado, sin efecto retroactivo."
Perú	Art. 5, LPDP. "[P]ara el tratamiento de los datos personales debe mediar el consentimiento del titular."	SI. Art. 13.5, LPDP. "El consentimiento debe ser previo, informado, expreso e inequívoco".	NO.	NO.	SI.	NO.	SI. 13.6, LPDP. "En el caso de datos sensibles, el consentimiento para efectos de su tratamiento, además debe efectuarse por escrito".	NO.	SI. Art. 13.5, LPDP. "Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto".	SI. Art. 13.5, LPDP. "El consentimiento debe ser previo, informado, expreso e inequívoco".	SI. Art. 13.5, LPDP. "El consentimiento debe ser previo, informado, expreso e inequívoco".	NO.	SI. Art. 13.7, LPDP. "El titular de datos personales puede revocar su consentimiento en cualquier momento, observando al efecto los mismos requisitos que

													con ocasión de su otorgamiento".
República Dominicana	SI. Art. 5, núm. 4. Consentimiento del afectado. "El tratamiento y la cesión de datos personales es ilícito cuando el titular de los datos no hubiere prestado su consentimiento libre, expreso y consciente, que deberá constar por escrito o por otro medio que permita que se le equipare, de acuerdo a las circunstancias..."	SI. Expresa y destacada. Art. 5, núm. 4. "libre, expreso y consciente, que deberá constar por escrito o por otro medio que permita que se le equipare, de acuerdo a las circunstancias... "	NO.	NO. Consciente.	NO.	NO.	SI. Art. 5, núm. 4. "libre, expreso y consciente, que deberá constar por escrito o por otro medio que permita que se le equipare, de acuerdo a las circunstancias... "	SI. Art. 5, núm. 4.- "libre, expreso y consciente, que deberá constar por escrito o por otro medio que permita que se le equipare, de acuerdo a las circunstancias". El referido consentimiento, prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de los datos descritos en el numeral 3 del presente artículo".	SI. Consentimiento del afectado y del titular.	SI. Art. 6. Definiciones: "Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernen".	SI. Art. 5, núm. 3. Derecho de información. "Cuando se recaben datos personales que requieran del consentimiento del titular de los datos, para que se les pueda dar el tratamiento de datos o ser cedidos después de obtener dicho consentimiento, se deberá informar previamente, a por lo menos uno de los titulares de los datos, en forma expresa y clara".	SI. Art. 28. Cesión. "Los datos personales objeto de tratamiento de datos sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario, con el previo consentimiento de por lo menos uno de los titulares de los datos".	NO.
Uruguay	SI. Manifestación de voluntad. Art. 4, Ley 18.331. Definiciones. Consentimiento del titular: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierne.	SI. Art. 9°, Ley 18.331. Principio del previo consentimiento informado. El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá	NO. Destacada El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y **destacada,** previa notificación al requerido de datos, de la información	SI.	SI.	SI.	NO.	SI. Art. 9, Ley 18.331. "Deberá documentarse".	SI. Art. 9°, Ley 18.331. Principio del previo consentimiento informado. "El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse".	SI. Art. 5, D), Ley 18.331. Previo consentimiento informado. Art. 9°. Principio del previo consentimiento informado.	SI. Art. 9, Ley 18.331. Principio del previo consentimiento informado. "El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el	SI. Art. 8°, Ley 18.331. "Tampoco podrán comunicarse datos entre bases de datos, sin que medie ley o previo consentimiento informado del titular". Art. 17, Ley 18.331. "Derechos referentes a la comunicación de datos.- Los datos personales objeto de tratamiento sólo	SI. Art. 17, Ley 18.331. "Derechos referentes a la comunicación de datos.- [...] El previo consentimiento para la comunicación es revocable".

documentarse.	descrita en el artículo 12 de la presente ley.	que deberá documentarse”.	podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo”.

Fuente y elaboración: La autora (2018).

El consentimiento es el principio más importante de la protección de datos personales; por eso todos los países que reconocen este derecho fundamental incluyen este principio: Argentina, Brasil, Colombia, Costa Rica, Ecuador, Guatemala, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay. De los cuales, Colombia menciona el término "autorización", mientras que Nicaragua, Uruguay y Panamá mencionan "manifestación de la voluntad", pero en todos el consentimiento del titular libre de vicios es el objetivo.

Las características del consentimiento varían entre los siguientes:

- Expreso: Argentina, Colombia, Costa Rica, Guatemala, México, Perú, República Dominicana y Uruguay. Argentina y República Dominicana señalan que junto con otras declaraciones, el consentimiento deberá figurar en forma expresa y destacada. Nicaragua usa el término inequívoco para suplir la característica de expreso.

  Ecuador determina que es expreso, pero la norma que lo señala es sectorial ya que solo regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, por medio de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas, conforme el artículo 1 de la Ley de comercio electrónico, firmas electrónicas y mensajes de datos.

- Tácito: Únicamente México acepta el consentimiento tácito en su normativa.
- Específico: Brasil, México, Nicaragua, Panamá, República Dominicana y Uruguay. República Dominicana usa el criterio "consciente". Costa Rica usa el término "preciso".
- Inequívoco: Es decir, que no cabe duda de la manifestación de voluntad. Brasil, Costa Rica, Nicaragua, Panamá, Perú y Uruguay.
- Libre: Argentina, Brasil y Nicaragua
- Escrito: Argentina, Brasil, Costa Rica, Guatemala, México, Nicaragua, Perú y República Dominicana.
- No escrito: Colombia no solicita que el consentimiento sea escrito, sino que se realice por cualquier medio que pueda ser objeto de consulta posterior. Uruguay señala que el consentimiento expreso deberá documentarse.
- Otros medios: Argentina señala que además de consentimiento escrito puede serlo por otro medio equiparable, de acuerdo con las circunstancias; por su parte Costa Rica menciona medio físico o electrónico. México señala que el consentimiento debe ser por escrito o por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Nicaragua registra que el consentimiento deberá ser otorgado por escrito o por otro medio idóneo, físico o electrónico. Brasil señala que debe ser por escrito o por otros medios que demuestren la manifestación de voluntad. Panamá determina que la voluntad puede ser emitida de forma directa o a través de mandato, pero mandatario deberá respetar lo estipulado y se dejará constancia, por escrito o de forma electrónica, con la condición de que pueda. El medio escrito y los otros medios se usan generalmente como medios probatorios.
- Titular: La persona titular del derecho es la que puede consentir. Argentina, Brasil, Colombia, Costa Rica, Ecuador, Guatemala (ámbito público), México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay. En el caso de

Costa Rica y Nicaragua además se faculta expresamente también a los representantes legales o apoderados.

- Previo: Argentina, Ecuador, Guatemala (ámbito público) y Nicaragua no lo menciona. Colombia, Costa Rica, México, Perú, República Dominicana y Uruguay determinan la necesidad de que el consentimiento se obtenga mediante una información clara y completa realizada antes del consentimiento. Panamá señala de forma expresa que el consentimiento deber ser previo.
- Informado: Esto es que se informe al titular de las consecuencias de la entrega de sus datos; así lo señalan: Argentina, Brasil, Colombia, Costa Rica, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay.
- Cesión: Argentina, Brasil, Nicaragua, México, República Dominicana y Uruguay señalan que para la cesión es necesario el consentimiento previo del titular de los datos, al que se le debe informar sobre su finalidad de la transferencia y la identificación del cesionario. Solo México requiere adicionalmente que se informe sobre los mecanismos y medios disponibles para que el titular pueda manifestar su negativa para el tratamiento. Nicaragua y República Dominicana establecen que también podrán cederse si los fines están directamente relacionados con el interés legítimo del cedente y del cesionario. Panamá señala que para la cesión, los responsables del tratamiento de datos solo podrán transferir información sobre estos cuando cuenten con el consentimiento previo, informado e inequívoco del titular.

  Por su parte, Colombia, Costa Rica, Ecuador determinan la necesidad de que para la cesión exista consentimiento del titular o autorización legal. En el caso del Ecuador, la normativa sectorial aplicable permite que el titular escoja los datos a ser transferidos.

  Guatemala (ámbito público), Panamá y Perú no hacen alusión expresa a la cesión.

- Revocable: Argentina, Brasil, Costa Rica, Ecuador, México, Nicaragua, Panamá, Perú y Uruguay señalan que respecto de la cesión el consentimiento es revocable. Colombia, Guatemala (ámbito público) y República Dominicana no mencionan la revocabilidad. Únicamente México y Perú señalan que la revocabilidad puede producirse en cualquier momento. Siempre que se cumplan los mismos requisitos o de la misma forma en que se obtuvo la autorización, a decir de Perú y Costa Rica, o por escrito o cualquier medio equivalente al tenor de lo determinado por Nicaragua, o cumpliendo con cada uno de los criterios constantes en el aviso de privacidad como señala México. No es posible aplicar efecto retroactivo como señalan Costa Rica, Ecuador (norma sectorial), México y Nicaragua. Panamá señala en el artículo 6, numeral 4 que el consentimiento podrá ser revocado, sin efecto retroactivo.

1.5.4.7 Excepciones al consentimiento

Tabla 23

País	Consta descritas las excepciones al consentimiento
El Salvador	NO.
Bolivia	NO.
Chile	NO.
Honduras	NO.
Paraguay	NO.
Venezuela	NO.
Jamaica	Art. 19, núm. 2. La Constitución de Jamaica señala que ante la ausencia de consentimiento por parte de su titular, ninguna persona estará sujeta a la búsqueda de su persona o su propiedad o la entrada de otros en sus instalaciones a menos que: la ley autorice a través de disposiciones razonablemente basadas en: "a. en interés de la defensa, la seguridad pública, el orden público, la moralidad pública, la salud pública, los ingresos públicos, la planificación de la ciudad y el país o el desarrollo y la utilización de cualquier propiedad de manera que se promueva el beneficio público; [...] c. con el propósito de prevenir o detectar el crimen; o d. con el propósito de proteger los derechos o libertades de otras personas" (Traducido del inglés por la autora).

Fuente y elaboración: La autora (2018).

De lo señalado en el cuadro anterior, Jamaica es el único país que desde la perspectiva de protección de los datos mediante la privacidad que establece la necesidad de que sea la ley la que determine los casos en los que no es necesario el consentimiento.

a) Respecto del derecho a la protección de datos personales

Tabla 24

País	Excepciones al consentimiento (no será necesario el consentimiento)	Autorizado por ley								
		Fuentes acceso al público	Datos de naturaleza pública	Funciones propias de entidades estatales	Orden judicial	Defensa de derechos	Datos identificación o de registro civil	Relación jurídica	Relación profesional, científica o profesional	Operaciones de entidades financieras
Argentina	No será necesario el consentimiento.	Art. 5. a) Los datos se obtengan de fuentes de acceso público irrestricto. Archivos, registros o bancos de datos con fines de publicidad. Art. 26. Prestación de servicios de información crediticia. Art. 27. 1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público.	NO.	Art. 5. b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.	NO.	NO.	Art. 5. "c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio".	Art. 5. "d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento".	Art. 5. "d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento".	Ley 25.326, art. 5. "e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526". Art. 26. "5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios". Art. 26. 1. "En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público…"
Brasil	En lugar de establecerse excepciones al consentimiento el Art. 7 de la LGPD señala que el procesamiento de datos personales solo puede realizarse en los casos señalados por la ley.	Párrafo 3. El procesamiento de datos personales cuyo acceso es público considerará el propósito, la buena fe y el interés público que justificaron su disponibilidad. § 4 El requisito de consentimiento previsto en el contenido de este artículo no se aplica a los datos que el titular haga públicos de forma manifiesta, salvaguardando los derechos del titular y los principios previstos en esta Ley.	NO	Art. 26. El uso compartido de datos personales por parte del Gobierno debe cumplir propósitos específicos de ejecución de políticas públicas y atribución legal por parte de organismos y entidades públicas, respetando los principios de protección de datos personales enumerados en el art. 6 de esta Ley.	NO	NO	NO	NO	NO	NO
Colombia	No será necesario el consentimiento.	NO.	b) Datos de naturaleza pública.	Art. 10. Casos en que no es necesaria la autorización. La autorización del titular no será necesaria cuando se trate de: a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.	Art. 10. Casos en que no es necesaria la autorización. La autorización del titular no será necesaria cuando se trate de: a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.	NO.	e) Datos relacionados con el Registro Civil de las Personas.	NO.	NO.	NO.

Costa Rica	Conforme a lo expuesto en el artículo 5 de la Ley 8968, podrá tratarse datos cuando exista orden fundamentada dictada por una autoridad competente o acuerdo adoptado por una comisión especial de la Asamblea Legislativa; también cuando se trate de datos de acceso irrestricto y los datos deban ser entregados por disposición constitucional o legal. Art. 5, Ley 8968. "No será necesario el consentimiento expreso cuando: [...] c) Los datos deban ser entregados por disposición constitucional o legal".	Art. 5, Ley 8968. "b) Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general".	NO.	2. Datos personales de acceso restringido. Datos personales de acceso restringido son los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública. Su tratamiento será permitido únicamente para fines públicos o si se cuenta con el consentimiento expreso del titular.	Art. 5, Ley 8968. a) Exista orden fundamentada, dictada por la autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo.	NO.	NO.	NO.	NO.	NO.
Ecuador	Art. 9, LCEFEMD. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.	Art. 9, LCEFEMD. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público.	NO.	Art. 9, LCEFEMD. No será preciso el consentimiento para recopilar datos personales cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia.	NO.	NO.	NO.	Art. 9, LCEFEMD. No será preciso el consentimiento para recopilar datos personales cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.	NO.	NO.
Guatemala	Ley de Acceso a la Información Pública, art. 32. Excepción del consentimiento. No se requerirá el consentimiento del titular de la información para proporcionar los datos personales en los siguientes casos [...] 4. Los establecidos en esta ley; [...] 6. En los demás casos que establezcan las leyes.	NO.	NO.	2. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades del Estado, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;	3. Cuando exista una orden judicial.	NO.	5. Los contenidos en los registros públicos.	NO.	NO.	NO.
México	Art. 22, LPDPSO. "El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos: I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla..." Art. 8., LPDPP. Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente ley. Art. 10, LPDPP. No será necesario el consentimiento para el tratamiento de los datos personales cuando: I. Esté previsto en una ley. Art. 37, LPDPP. Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el	Art. 3. "Fuente de acceso público: Aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación, de conformidad con lo señalado por el Reglamento de esta Ley". Art. 10, LPDP. Los datos figuren en fuentes de acceso público. Art. 22 VIII. Cuando los datos personales figuren en fuentes de acceso público.	NO.	Art. 22, LPDPSO. II. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.	Art. 22, LPDPSO. III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente. Art. 10, LPDPP. VII. Se dicte resolución de autoridad competente.	Art. 22, LPDPSO. "IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente".	NO.	Art. 10, LPDP. "tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable". Art. 22, "V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable".	NO.	NO.

	consentimiento del titular cuando se dé alguno de los siguientes supuestos: I. Cuando la transferencia esté prevista en una ley o tratado en los que México sea parte.									
Nicaragua	Art. 6, Ley 787. Consentimiento. El titular de los datos deberá dar por sí o por su representante legal o apoderado el consentimiento para la entrega de los datos, salvo que la ley disponga otra cosa dentro de los límites razonables. La razonabilidad deberá ser considerada por la Dirección de Protección de Datos Personales, si se le planteare alguna controversia.	NO.	NO.	NO.	Art. 6. No será necesario el consentimiento cuando: a. Exista orden motivada, dictada por autoridad judicial competente.	NO.	Art. 6. No será necesario el consentimiento cuando: [...] d. Los datos se obtengan de fuentes de acceso público irrestricto y se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, y fecha de nacimiento".	Art. 6. No será necesario el consentimiento cuando: [...] c. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; y".	NO.	NO.
Panamá	El artículo 8 de la Ley 81 señala cuando no se requiere autorización para el tratamiento de datos personales. El numeral 4 del artículo 6, establece que es posible tratar datos por autorización de su titular o por autorización de la Ley, de tal manera que los casos anunciados en esta norma no son más que mandatos legales autorizando dicho tratamiento.	El artículo 8 de la Ley 81, no se requiere de autorización para el tratamiento de datos personales cuando estos: provengan o que se recolecten de fuentes de dominio público o accesible en medios públicos.	NO.	Artículo 8, numeral 2 de la Ley 81 señala que se requiere de autorización para el tratamiento de datos personales para el ejercicio de competencias de la Administración Pública	Artículo 13. Los datos sensibles no pueden ser objeto de transferencia, excepto en los casos siguientes: Cuando se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso con autorización judicial competente.	NO.	SI, Art. 8, numeral 4 de la Ley 81, "(...) Los que se contengan en listas relativas a una categoría de persona que se limiten a indicar antecedentes, como la pertenencia de la persona natural a una organización, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento	SI, Art. 8, numeral 9 de la Ley 81, "(...) El tratamiento que sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o lo derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un menor de edad i una persona con discapacidad.	SI,, Art. 8, numeral 4 de la Ley 81, "(...) Los que son necesarios dentro de una relación comercial establecida, ya que sea para atención directa, comercialización o venta de los bienes o servicios pactados	Art. 8, numeral 3 de la Ley 81, señala que los de carácter económico, financiero, bancario o comercial que cuenten con el consentimiento previo.

Perú	Limitaciones al consentimiento. Art. 14, LPDP. No se requiere el consentimiento del titular de datos personales, para el tratamiento de datos personales cuando: [...] k) Otros establecidos por ley, o por el respectivo reglamento.	Art. 14, LPDP. b) se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.	NO.	Art. 14, LPDP. a) los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.	NO.	Art. 14, LPDP. j) el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de datos personales.	NO.	Art. 14, LPDP. e) los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte.	Art. 14, LPDP. f) se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.	Art. 14, LPDP. c) se refiera a datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.
República Dominicana	Art. 27, Ley 172-13. Excepciones al requerimiento de consentimiento. No será necesario el consentimiento para el tratamiento y la cesión de datos cuando: [...] 6. Así lo disponga una ley.	Art. 27, Ley 172-13. 1. Se obtengan de fuentes de acceso público.		Art. 27, Ley 172-13 2. Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. [...] 7. Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias.	NO.	NO.	NO.	Art. 27, Ley 172-13 4. Se deriven de una relación comercial, laboral o contractual [...] con la persona física, y resulten necesarios para su desarrollo o cumplimiento.	Art. 27, Ley 172-13 4. Se deriven de una relación comercial, laboral o contractual, científica o profesional con la persona física, y resulten necesarios para su desarrollo o cumplimiento.	Art. 27, Ley 172-13 5. Se trate de datos personales que reciban de sus clientes en relación a las operaciones que realicen las entidades de intermediación financiera reguladas por la Ley Monetaria y Financiera y de agentes económicos, de las Sociedades de Información Crediticia (SIC), y de las entidades que desarrollan herramientas de puntajes de crédito para la evaluación del riesgo de los deudores del sistema financiero y comercial nacional, de acuerdo a las condiciones establecidas en el artículo 5, numeral 4.
Uruguay	Art. 9º, Ley 18.331. "No será necesario el previo consentimiento cuando..." Art. 17, Ley 18.331. "El previo consentimiento no será necesario cuando: Así lo disponga una ley de interés general".	Art. 9º, Ley 18.331. "No será necesario el previo consentimiento cuando: A) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación".		Art. 9º, Ley 18.331. "No será necesario el previo consentimiento cuando: [...] B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".	NO.	NO.	Art. 9º, Ley 18.331. "No será necesario el previo consentimiento cuando: [...] C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha	Art. 9º, Ley 18.331. "No será necesario el previo consentimiento cuando: [...] D) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento".	Art. 9º, Ley 18.331. "No será necesario el previo consentimiento cuando: [...] D) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento".	NO.

							de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma".			

País	Autorizado por ley									
	Promoción y competencia	Defensa Nacional o Seguridad pública y represión de delitos	Autoridades administrativas y judiciales	Salud	Organismos sin fin de lucro	Urgencia sanitaria y de bienes	Fines estadísticos, históricos y científicos	Disociación	Persona desaparecida	Uso doméstico
Argentina	NO.	Ley 25.326, art. 23, "2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad. 3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".	Art. 23. "para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales".	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Brasil	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Colombia	NO.	NO.	NO.	c) Casos de urgencia médica o sanitaria.	NO.	NO.	d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.	NO.	NO.	NO.
Costa Rica	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Ecuador	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Guatemala	NO.	NO.	NO.	NO.	NO.	NO.	NO.	1. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por	NO.	NO.

								el cual no puedan asociarse los datos personales con el individuo a quien se refieran.		
México	NO.	NO.	NO.	Art. 10, LPDP. "sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o se dicte resolución de autoridad competente". Art. 22, "VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria".	NO.	Art. 10, LPDP. "exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes". Art. 22. VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.	NO.	Art. 10, LPDP. "los datos personales se sometan a un procedimiento previo de disociación". IX. Cuando los datos personales se sometan a un procedimiento previo de disociación.	Art. 22, LPDPSO. "X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.	NO.
Nicaragua	NO.	Art. 24. Excepcionalidad en el uso de los datos personales. La colecta y el tratamiento de datos personales con fines de seguridad y defensa nacional o seguridad pública por parte de los órganos de inteligencia de la Policía Nacional y el Ejército de Nicaragua, sin consentimiento de los titulares, queda limitado a lo necesario para el estricto cumplimiento de las misiones legalmente asignadas para la seguridad nacional, defensa nacional, seguridad pública o para la investigación de los delitos conforme lo establecido en la Constitución Política de la República de Nicaragua y leyes de la materia. Los ficheros de datos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad. Los datos personales obtenidos para fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su registro.	NO.	NO.	NO.	Art. 6. No será necesario el consentimiento cuando: [...] b. Los datos personales se sometan a un procedimiento previo de disociación.	NO.	NO.	NO.	NO.
Panamá	NO.		NO.	Art. 8, numeral 9, Ley 81,"(…) Cuando el consentimiento se refiera a datos personales sensibles de salud, el consentimiento será previo, irrefutable y expreso	SI, Art. 8 numeral 6 Ley 81, "(…) El tratamiento de datos personales que realicen organizaciones privadas para el uso exclusivo de sus asociados y de las entidades a que	SI, Art. 8, numeral 7, Ley 81, "(…) Los casos de urgencia médica o sanitaria.	SI, Art. 8 numeral 8 Ley 81, "(…). El tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos	NO.	NO.	NO.

					están afiliadas, con fines estadísticos, de tarificación u otro de beneficio general de aquellos (...)"		Artículo 12. En el caso de tratamiento posterior de os datos con fines de investigación, estudios o encuestas o conocimiento de interés público, no será necesario el consentimiento del titular de los datos, siempre que estos sean anonimizados por el responsable de su custodia o tratamiento.			
Perú	Art. 14, LPDP. "4. Cuando medie norma para la promoción de la competencia [...] siempre que la información no sea utilizada en perjuicio de la privacidad del usuario".	Art. 13. "13.8. El tratamiento de datos personales relativos a la comisión de infracciones penales o administrativas solo puede ser efectuado por las entidades públicas competentes, salvo convenio de encargo de gestión conforme a la Ley 27444, Ley de Procedimiento administrativo General, o la que haga sus veces. Cuando se haya producido la cancelación de los antecedentes penales, judiciales, policiales y administrativos, estos datos no pueden ser suministrados salvo que sean requeridos por el Poder Judicial o el Ministerio público, conforme a Ley".	NO.	Art. 14, LPDP. "6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular..."	Art. 14 LPDP. "7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos".	NO.	NO.	Art. 14, LPDP. i) se hubiera aplicado un procedimiento de anonimización o disociación.	NO.	NO.
República Dominicana	Art. 27. Ley 172-13. "3. Se trate de listas para fines mercadológicos, cuyos datos se limiten a nombre, cédula de identidad y electoral, pasaporte, identificación tributaria y demás informaciones	NO.	NO.	Art. 27, Ley 172-13. "8. Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve el secreto de la identidad de los titulares de los datos mediante mecanismos de disociación adecuados".	NO.	NO.	NO.	Art. 27, Ley 172-13. 9. Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.	NO.	NO.

	biográficas".									
Uruguay	NO.	Art. 25, Ley 18.331. "Base de datos correspondientes a las Fuerzas Armadas, Organismos Policiales o de Inteligencia.- Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en las bases de datos de las fuerzas armadas, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichas bases de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, organismos policiales o inteligencia, sin previo consentimiento de los titulares, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Las bases de datos, en tales casos, deberán ser específicas y establecidas al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".	NO.	Art. 17, Ley 18.331. "El previo consentimiento no será necesario cuando: [...] C) Se trate de datos personales relativos a la salud y sea necesario por razones de salud e higiene públicas, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados".	NO.	NO.		NO.	NO.	Art. 9º, Ley 18.331. "No será necesario el previo consentimiento cuando: [...] E) Se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico".

Fuente y elaboración: La autora (2018).

Sobre “excepciones al consentimiento” no será necesario el consentimiento para la recopilación y tratamiento de la información; Los demás países, Argentina, Colombia, Costa Rica, Ecuador, Guatemala (ámbito público), México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay determinan la necesidad de mandato legal o disposición legal expresa que permita suplir la autorización o consentimiento del titular.

En el caso de Brasil, no se establecen excepciones al consentimiento sino que el artículo 7 de la LGPD señala que el procesamiento de datos personales solo puede realizarse en los casos señalados por la ley. De esta manera, la ley determina los casos en los que es procedente el tratamiento y el consentimiento es uno más de los supuestos considerados lícitos o legítimos.

A continuación se analizan los casos exceptuados de receptar el consentimiento.

- *Fuentes de acceso al público:* Argentina, Brasil, Costa Rica, Ecuador, México, Panamá, Perú, República Dominicana y Uruguay establecen que los datos contenidos en fuentes de acceso público no requieren consentimiento del titular. Colombia, Guatemala (ámbito público) y Nicaragua no han establecido esta salvedad. Marca elemento diferenciador lo señalado en la norma mexicana, pues determina no solo la condición de constar en un registro accesible al público, sino que son fuentes accesibles, aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación (art. 3, LPDPSO).

- *Datos de naturaleza pública:* únicamente Colombia menciona este tipo de datos utilizando el término público desde la perspectiva de notoriedad o publicidad, por eso utiliza el término naturaleza para darle este enfoque distinto de los datos públicos que son aquellos generados por el Estado en sus procesos de gestión de actividades y recursos institucionales.

- *Funciones propias de entidades estatales:* son aquellas que pueden recabarse sin autorización del titular para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal conforme señala Argentina y Uruguay. Otros países solo mencionan de manera general las funciones o competencias de las entidades estatales como: Colombia, Ecuador, Guatemala, Panamá, Perú y República Dominicana. Costa Rica utiliza el término “fines de las instituciones públicas”. México hace alusión a “competencias propias, compatibles y análogas”; de esta manera amplía el ámbito de acción de las entidades estatales. Brasil señala la ejecución de políticas públicas y atribución legal.

- *Orden judicial:* Colombia, Costa Rica, Guatemala, México, Nicaragua establecen que puede obviarse la autorización del titular cuando exista orden

judicial. Costa Rica, México y Nicaragua exigen además que la orden sea motivada. México y Costa Rica señalan que la orden, resolución o mandato puede provenir además de autoridad judicial, así como de autoridad competente. Además, Costa Rica señala que puede originarse de acuerdo a lo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo. Panamá señala que cuando se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso con autorización judicial competente.

- *Defensa de derechos:* únicamente México y Perú determinan que podrá recopilarse y tratarse datos personales sin autorización del titular para salvaguardar intereses legítimos del titular de datos personales o para el reconocimiento o defensa de derechos del titular ante autoridad competente.

- *Datos de identificación o de registro civil:* Argentina, Nicaragua y Uruguay establecen que cuando se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio para la recolección y el tratamiento no es necesario consentimiento del titular. Uruguay incluso aclara que lo mismo ocurre con las personas jurídicas y sus datos relativos a razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma. Colombia señala de manera general aquellos datos relativos a registro civil; y Guatemala, por su parte, determina aquellos datos que consten en registros públicos.

  Panamá determina aquellos que se contengan en listas sobre antecedentes, pertenencia a una organización, profesión o actividad, títulos educativos, dirección o fecha de nacimiento. Si bien, no son datos civiles son importantes para el desarrollo de las actividades de los titulares.

- *Relación jurídica:* Argentina, México, Nicaragua, Perú, República Dominicana y Uruguay señalan que no es necesario el consentimiento para el tratamiento de datos personales cuando se deriven de una relación contractual, comercial o laboral del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; es decir que tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable. Ecuador, por su parte, desarrolla el mismo contenido precisando relaciones laborales y administrativas, solo que limitado a un ley sectorial aplicable a relaciones de e-*comerce*.

  Panamá, determina el tratamiento sin necesidad de consentimiento cuando sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

- *Relación profesional, científica o profesional:* Argentina, Panamá, Perú, República Dominica y Uruguay señalan que no será necesario el consentimiento para tratar datos personales que se deriven de una relación científica o profesional con la persona física, y resulten necesarios para su desarrollo o cumplimiento. Por su parte, en Panamá no se requiere consentimiento para los datos personales necesarios en una relación comercial establecida, ya que sea para atención directa, comercialización o venta de los bienes o servicios pactados.

- *Operaciones de entidades financieras:* Argentina, Perú y República Dominicana señalan que no es necesario consentimiento para tratar, ceder, datos cuando se usen para operaciones que realicen las entidades financieras; es decir, la prestación de servicios de información crediticia cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios. Argentina aclara que en la prestación de servicios de información crediticia solo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público. El resto de países, incluidos México y Uruguay, no permiten esta salvedad. Panamá menciona que no se requiere de autorización para el tratamiento de datos personales los de carácter económico, financiero, bancario o comercial que cuenten con el consentimiento previo.

- *Promoción y competencia:* Perú determina que pueden tratarse, sin consentimiento del titular, aquellos datos personales cuando medie norma para la promoción de la competencia siempre que la información no sea utilizada en perjuicio de la privacidad del usuario. Mientras que República Dominicana sostiene que cuando se trate de listas para fines mercadológicos, cuyos datos se limiten a nombre, cédula de identidad y electoral, pasaporte, identificación tributaria y demás informaciones biográficas, esta última. Ninguno de los otros países analizados permiten esta excepción.

- *Defensa nacional o seguridad pública y represión de delitos:* Argentina, Nicaragua y Uruguay señalan que se releva de autorización del titular el tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados; queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquellos para la defensa nacional, la seguridad pública o para la represión de los delitos. Deberá existir una clasificación y los archivos; en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad. Los datos personales registrados con fines policiales se

cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. Perú, por su parte, señala que el tratamiento de datos personales relativos a la comisión de infracciones penales o administrativas solo puede ser efectuado por las entidades públicas competentes, salvo convenio de encargo de gestión conforme a la Ley 27444. Cuando se haya producido la cancelación de los antecedentes penales, judiciales, policiales y administrativos, estos datos no pueden ser suministrados salvo que sean requeridos por el Poder Judicial o el Ministerio público, conforme a la ley.

- *Autoridades administrativas y judiciales:* Únicamente, Argentina señala que será posible no tomar consentimiento del titular del dato para fines administrativos, cuando deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales. Es decir, aquellos datos de seguridad nacional pero que por disposición de ley deben estar en conocimiento de autoridades administrativas o judiciales. Panamá señala que no se requiere de autorización para el tratamiento de datos personales para el ejercicio de competencias de la Administración Pública.

- *Salud:* México señala que pueden tratarse datos personales sin autorización del titular en casos de urgencia médica o sanitaria. Perú, República Dominicana y Uruguay, por su parte, determinan esta excepción cuando sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento en los términos que establece la Ley General de Salud, y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o se dicte resolución de autoridad competente. Uruguay, sin embargo, aclara además que es necesario que para este tratamiento se preserve el secreto de la identidad de los titulares de los datos mediante mecanismos de disociación adecuados. Panamá respecto de salud requiere de consentimiento previo, irrefutable y expreso.

- *Organismos sin fin de lucro:* Perú es el único país que permite que el tratamiento sin autorización del titular sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.

- *Urgencia sanitaria y de bienes:* México y Nicaragua determinan la excepción del solicitar consentimiento del titular cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes. Panamá señala que no se requiere de autorización para el tratamiento de datos personales en caso de urgencia médica o sanitaria,

- *Fines estadísticos, históricos y científicos:* Colombia señala que no será necesario el consentimiento para tratar datos personales cuando autorizado por la ley para fines históricos, estadísticos y científicos. Es el único país analizado que opta por este sistema, la mayoría orienta su normativa a la disociación de este tipo de datos. Panamá señala que para fines históricos o científicos, no es necesario el consentimiento, siempre que estos sean anonimizados por el responsable de su custodia o tratamiento.

- *Disociación:* No se requiere autorización del titular cuando se van a tratar datos anonimizados, conforme las normativas de Guatemala, México, Perú y República Dominicana. Guatemala también señala que de esta manera, es decir disociado, deben tratarse los datos que deben usarse para estadísticas, científicas o de interés general.

- *Persona desaparecida:* México establece que no se requiere de autorización del titular para el tratamiento de datos cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

- *Uso doméstico:* Uruguay, por su parte, señala que no será necesario el consentimiento previo cuando se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico.

Tabla 25

	Excepciones al consentimiento para la cesión de datos personales							
	Autorizados por ley (referencia a normativa de excepciones al consentimiento)	**Fuentes accesibles al público**	**Autorizado por mandato judicial**	**Relación jurídica**	**Relaciones profesionales y científicas**	**Operaciones financieras**	**Promoción y competencia**	**Funciones propias de entidades estatales**
Argentina	Ley 25.326, art. 11. Sobre cesión: "3. El consentimiento no es exigido cuando: a) Así lo disponga una ley; b) En los supuestos previstos en el artículo 5º inciso 2". Art. 5. "2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto".	Art. 5. "2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; [...] c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio..."	NO.	Art. 11. Sobre cesión: 3. b. Art. 5. 2. "d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento".	Art. 11 Sobre cesión: 3. b. Art. 5. 2. "d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento".	Art. 11. Sobre cesión: 3. b. Art. 5. 2. "e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526".	NO.	Art. 11. "c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias". Art. 11. Sobre cesión: 3. b. Art. 5. 2. "b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".
Brasil	Por cuanto, esta normativa no establece excepciones al consentimiento sino causas legítimas o lícitas de tratamiento, al tenor del Art. 7 de la LGPD, tampoco se aplica la excepción al consentimiento para la cesión de datos personales.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Colombia	Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.	NO.	Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.	NO.	NO.	NO.	NO.	NO.
Costa Rica	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Ecuador	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Guatemala	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
México	Art 66, LPDPSO. "Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las	NO.		Art. 70, LPDPSO. "VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular". Art. 70. "VII. Cuando la transferencia sea necesaria por	NO.	NO.	NO.	Art. 70, LPDPSO. "El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos: I. Cuando la transferencia esté prevista en esta Ley u otras leyes, convenios o Tratados Internacionales suscritos y

	partes". Lo dispuesto en el párrafo anterior, no será aplicable en los siguientes casos: Art. 66. I. Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos, o Art. 70. VIII. Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la presente ley.			virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero". Art. 37. "IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero". Art. 37. "VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular".				ratificados por México".
Nicaragua		NO.	NO.	NO.	NO.	NO.	NO.	
	Art. 13. Cesión y transferencia de datos personales. Este (consentimiento) no podrá ser exigido cuando lo disponga una ley.							Art. 13. Cesión y transferencia de datos personales. Este (consentimiento) no podrá ser exigido cuando se realice entre instituciones del Estado en el ejercicio de sus atribuciones.
Panamá	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
República Dominicana	Art. 27, Ley 172-13. "Excepciones al requerimiento de consentimiento. No será necesario el consentimiento para el tratamiento y la cesión de datos cuando: [...] 6. Así lo disponga una ley".	Art. 27, Ley172-13. "1. Se obtengan de fuentes de acceso público".			Art. 27, Ley 172-13. "4. Se deriven de una relación comercial, laboral o contractual, científica o profesional con la persona física, y resulten necesarios para su desarrollo o cumplimiento".	Art. 27, Ley 172-13. "5. Se trate de datos personales que reciban de sus clientes en relación a las operaciones que realicen las entidades de intermediación financiera reguladas por la Ley Monetaria y Financiera y de agentes económicos, de las Sociedades de Información Crediticia (SIC), y de las entidades que desarrollan herramientas de puntajes de crédito para la evaluación del riesgo de los deudores del sistema financiero y comercial nacional, de acuerdo a las condiciones establecidas en el Artículo 5, numeral 4".	Art. 27, Ley 172-13. "3. Se trate de listas para fines mercadológicos, cuyos datos se limiten a nombre, cédula de identidad y electoral, pasaporte, identificación tributaria y demás informaciones biográficas".	Art. 27, Ley 172-13. "2. Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. [...] 7. Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias".
Uruguay	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Excepciones al consentimiento en la cesión de datos personales								

País	Interés público	Defensa Nacional o seguridad pública	Transferencia internacional o a organismos internacionales	Salud	Disociación	Investigación delito	Defensa de derechos	Sociedades controladas subsidiarias o afiliadas
Argentina	NO.	NO.	NO.	Art. 11. "d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados".	Art. 11. "e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables".	NO.	NO.	NO.
Colombia	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Costa Rica	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Ecuador	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Guatemala	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
México	Art. 37. "V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia".	Art. 70, LPDPSO. "IX. Cuando la transferencia sea necesaria por razones de seguridad nacional".	Art. 66, LPDPSO. "II. Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente". Art. 70, LPDPSO. "V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados". Art. 37, LPDPP. "II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios".	NO.	Art. 70, LPDPSO. "II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales; Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia".	Art. 70, LPDPSO. "IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última". Art. 37. "VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial".	Art. 37. "III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas".

Nicaragua	Art. 13. Cesión y transferencia de datos personales. Este (consentimiento) no podrá ser exigido cuando se trate de interés social, de seguridad nacional.	Art. 13. Cesión y transferencia de datos personales. Este (consentimiento) no podrá ser exigido cuando se trate de interés social, de seguridad nacional.	NO.	Art. 13. Cesión y transferencia de datos personales. Este (consentimiento) no podrá ser exigido cuando se trate de razones de salud pública.	Art. 13. Cesión y transferencia de datos personales. Este (consentimiento) no podrá ser exigido cuando se hubiere aplicado un procedimiento de disociación de datos, de modo que no se pueda atribuir a una persona determinada.	NO.	NO.	NO.
Panamá	NO.							
Perú	NO.							
República Dominicana	NO.	NO.	NO.	Art. 27, Ley 172-13 8. Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve el secreto de la identidad de los titulares de los datos mediante mecanismos de disociación adecuados.	Art. 27, Ley 172-13. "9. Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables".	NO.	NO.	NO.
Uruguay	NO.	NO.	NO.	NO.	Art. 17, Ley 18.331. El previo consentimiento no será necesario cuando: "D) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables".	NO.	NO.	NO.

Fuente y elaboración: La autora (2018).

Respecto de la autorización del titular para el tratamiento de datos personales, especial mención merece la autorización para la cesión que también puede ser exceptuada en varios casos que analizaremos a continuación:

- *Autorizados por ley (referencia a normativa de excepciones al consentimiento):* Argentina, México, Nicaragua, República Dominicana establecen por ley los casos en los que el consentimiento para la cesión está exceptuado. Otros países como Costa Rica, Ecuador, Guatemala, Panamá, Perú y Uruguay no realizan mención expresa. Brasil establece un sistema basado en la legitimidad y licitud del tratamiento en el que el consentimiento es uno más de los supuestos previstos en la ley, por lo que no existe referencia al consentimiento para la cesión.
- *Fuentes accesibles al público:* Solo Argentina y República Dominicana establecen la excepción del consentimiento para la cesión de datos personales cuando provengan de fuentes accesibles al público.
- *Autorizado por mandato judicial:* Colombia es el único país que establece esta excepción.
- *Relación jurídica:* Argentina y México establecen la salvedad de la autorización para la cesión cuando los datos personales provengan de relaciones contractuales previas o relaciones jurídicas que para su ejecución necesitan de esta información.
- *Relaciones profesionales y científicas:* Argentina y República Dominicana señalan la omisión de la autorización para la cesión cuando los datos personales provienen de relaciones profesionales y científicas que requieren de esos datos para su consecución.
- *Operaciones financieras:* Argentina y República Dominicana señalan que puede omitirse el consentimiento para la cesión cuando provienen de relaciones propias de operaciones financieras.
- *Promoción y competencia:* República Dominicana establece que cuando se trate de listas para fines mercadológicos, cuyos datos se limiten a nombre, cédula de identidad y electoral, pasaporte, identificación tributaria y demás informaciones biográficas se releva la autorización del titular en caso de cesión.
- *Funciones propias de entidades estatales:* Argentina y República Dominicana establecen expresamente la omisión de autorización del titular para la cesión en los casos de utilizar los datos para el ejercicio de las competencias propias de las entidades estatales.
- *Interés público:* Argentina, México, Nicaragua y República Dominicana establecen que no debe solicitarse autorización del titular para la cesión de datos personales cuando prima el interés social, público o de orden público.
- *Defensa nacional o seguridad pública:* México y Nicaragua relevan de autorización del titular el tratamiento de datos por cesión cuando se refieren a usos relativos a seguridad nacional.
- *Transferencia internacional o a organismos internacionales:* Solamente México establece que cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquellas que dieron origen al tratamiento del responsable transferente.

- *Salud:* Por cuestiones de salud pública, emergencia sanitaria, diagnóstico, entre otros, se releva el consentimiento del titular para la cesión de datos en los casos de Argentina, México, Nicaragua y República Dominicana.
- *Disociación:* Si los datos están disociados, es decir no vinculados al titular, se puede tratar incluso para la cesión sin autorización del titular; tal es el caso de Argentina, Nicaragua y República Dominicana.
- *Investigación delito:* México es el único país que establece esta salvedad en la excepción asociada a la investigación de delitos por parte de entidades autorizadas legalmente.
- *Defensa de derechos:* México establece que no se requerirá autorización para la cesión en caso de necesitar datos para la defensa de derechos de las personas.
- *Sociedades controladas subsidiarias o afiliadas:* Únicamente México establece que puede omitirse la autorización del titular para ceder datos, cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas.

1.5.4.8 Otros principios reconocidos en las normativas latinoamericanas

Desde esta perspectiva, se colige lo siguiente:

Tabla 26

País	Otros principios
El Salvador	NO.
Bolivia	NO.
Chile	Confidencialidad de recetas médicas. Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados.
Honduras	NO.
Paraguay	NO.
Venezuela	NO.

Fuente y elaboración: La autora (2018).

Se desprende de la tabla 26 que únicamente Chile establece un principio de confidencialidad dirigido exclusivamente a recetas médicas y análisis o exámenes de laboratorio; es decir, asociado a la salud de cada persona.

b) Respecto del derecho a la protección de datos personales

Tabla 27

País	Otros principios					
	Licitud	**Principio de utilización no abusiva**	**Principio de cesión**	**Integridad**	**Responsabilidad y rendición de cuentas**	**Principio de acceso y circulación restringida**
Argentina	Capítulo II, denominado principios generales relativos a la protección de datos personales, en el artículo 3 LPDP. Por el cual, la formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y reglamento pertinente. Esta licitud también se verifica al establecer la obligación de que los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.	Por cuanto el inciso 3 del artículo señala que los datos personales no podrán ser tratados con finalidades distintas o incompatibles con aquellas que motivaron su obtención se comprende que se incorpora en la legislación argentina el principio de utilización no abusiva.	Consta en el artículo 11, LPDP, que es parte del capítulo de principios generales relativos a la protección de datos personales el principio de cesión, mediante el cual los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, a quien se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.	NO.	NO.	NO.
Brasil	SI, Art. 7 LGPD cuando menciona la lista de requisitos y supuestos para que el tratamiento pueda realizarse	NO	NO	NO	SI, Principio de Responsabilidad y rendición de cuentas:: Art. 6 numeral X LGPD.- "(…) Rendición de cuentas y rendición de cuentas: Demostración por parte del agente de la adopción de medidas efectivas capaces de demostrar el cumplimiento y el cumplimiento de las normas de protección de datos personales, incluida la efectividad de dichas medidas".	SI, Art. 9 LGPD "El titular tiene derecho a un fácil acceso a la información sobre el procesamiento de sus datos, que debe estar disponible de manera clara, apropiada y abierta sobre, entre otras características previstas en la regulación para cumplir con el principio de libre acceso (…)"
Colombia	NO.	NO.	NO.	El principio denominado integridad, por el cual "se prohíbe que el manejo de los datos fuese incompleto, en razón a que esta situación puede distorsionar la veracidad de la información.	NO.	Principio de acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados conforme a la presente.
Costa Rica	NO.	NO.	NO.	NO.	NO.	NO.
Ecuador	NO.	NO.	NO.	NO.	NO.	NO.
Guatemala	NO.	NO.	NO.	NO.	NO.	NO.

México	Principio de licitud. La LFPDPPP de 2010 señala entre los principios aplicables el de licitud (art. 6), por el cual, los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta ley y demás normatividad aplicable. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos (art. 7).	NO.	NO.	NO.	Responsabilidad. La LFPDPPP de 2010 señala entre los principios aplicables el de responsabilidad (art. 6). La LGPDPPSO de 2017 señala el principio de responsabilidad, por el cual el responsable debe elaborar y revisar periódicamente políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable, y asignar recursos para su ejecución, así como servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología; poner en práctica un programa de capacitación y actualización; establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales; establecer procedimientos para recibir y responder dudas y quejas de los titulares (art. 30).	NO.
Nicaragua	NO.	NO.	NO.	NO.	NO.	NO.
Panamá	Art. 2, numeral 8 de la Ley 81 señala que Principio de licitud: para que el tratamiento de un dato personal sea licito, deberá ser recolectado y tratado con el consentimiento previo, informado e inequívoco del titular del dato o por fundamento legal.	NO.	NO.	NO.	NO.	NO.
Perú	Según el artículo 4, relativo al principio de legalidad, el tratamiento de los datos personales se hace conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.	NO.	NO.	NO.	NO.	NO.
República Dominicana	NO.	NO.	NO.	NO.	NO.	NO.
Uruguay	Principio de legalidad. Según la Ley 18.331, la formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia. Las bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública (art. 6º). Así, se entiende como	NO.	NO.	NO.	Según la Ley 18.331, el principio de responsabilidad se refiere a que el responsable de la base de datos lo es en la violación de las disposiciones de la presente ley (art. 12).	NO.

	principio de legalidad lo que en otras obligaciones se reconoce como obligación de registro de bases de datos y que va de la mano del derecho de consulta.

Fuente y elaboración: La autora (2018).

Tabla 28

País	Otros principios										
	Principio de proporcionalidad	**Principio de disposición**	**Principio de nivel de protección adecuado**	**Principio de Lealtad**	**Principio de veracidad**	**Principio de reserva**	**Principio acceso gratuito**	**Principio de prevención**	**Principio de no discriminación**	**Principio de necesidad**	**Principio de portabilidad**
Argentina	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Brasil	NO	NO	NO	NO	NO	NO	SI, Art. 6 numeral IV "(…) acceso gratuito: garantía a los titulares, consulta gratuita y fácil sobre la forma y duración del tratamiento, así como la integridad de sus datos personales; (…)"	SI, Art. 6 numeral IX "(…) no discriminación: la imposibilidad de llevar a cabo el tratamiento con fines discriminatorios ilícitos o abusivos;	SI, Art. 6 numeral VIII "(…) prevención: adopción de medidas para prevenir la ocurrencia de daños debido al procesamiento de datos personales;	SI, Art. 6 numeral III "(…) necesidad: limitación del tratamiento al mínimo necesario para el cumplimiento de sus propósitos, con la exhaustividad de los datos relevantes, proporcionales y no excesivos en relación con los propósitos del procesamiento de datos;(…)"	
Colombia	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Costa Rica	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Ecuador	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Guatemala	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
México	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Nicaragua	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Panamá	Art.2, numeral 3 de la Ley 81 señala que el principio de proporcionalidad: solo deberán ser solicitados aquellos datos adecuados, pertinentes y limitados al mínimo necesario en	NO.	NO.	Art.2, numeral 1 de la Ley 81 señala que el principio de lealtad: los datos personales deberán recabarse sin engaño o falsedad	Art.2, numeral 4 Ley 81 señala el principio de veracidad y exactitud: los datos de carácter personal serán exactos y puestos al	NO.	NO.	NO.	NO.	NO.	Art. 2 numeral 9 Ley 81 "(…) Principio de portabilidad: el titular de los datos tiene derecho a obtener de parte del responsa

	relación con la finalidad para la que son requeridos.			y sin utilizar medios fraudulentos, desleales o ilícitos.	día de manera que responda n con veracidad a la situación actual del propietario del dato...						ble del tratamiento una copia de los datos personales de manera estructurada en un formato y de uso común.
Perú	En el artículo 7, respecto del principio de proporcionalidad, se determina que todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.	El artículo 10, sobre el principio de disposición de recurso, señala que todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.	El artículo 11, sobre el principio de nivel de protección adecuado, aplicable al flujo transfronterizo de datos personales, señala que garantiza se un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta ley o por los estándares internacionales en la materia.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
República Dominicana	NO.	NO.	NO.	El artículo 5 de la Ley 172-13 describe otro principio directamente relacionado que es el de lealtad, por el cual se impone la prohibición de recoger los datos por medios fraudulen	NO.	NO.	NO.	NO.	NO.	NO.	NO.

				tos, desleales o ilícitos.							
Uruguay	NO.	NO.	NO.	Esta norma también menciona que la recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley; contenido que es propio del principio de legalidad o licitud, pero que consta incluido en este denominado principio de veracidad.	No consta en la Ley 18.331, el principio de calidad sino que un contenido equivalente al mismo, aparece denominado como principio de veracidad. Por el cual, para tratar datos personales deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. En consecuencia, los datos deberán ser exactos y es de cargo de responsable actualizarlos de ser necesario, si ha constatado la inexactitud o falsedad de los datos, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo,	En la legislación uruguaya aparece como principio de reserva lo que en otras normativas consta como derecho de confidencialidad. La Ley 18.331 señala que aquellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros no solo del responsable, sino de sus empleados aun cuando ya no sean parte de la entidad. Esta obligación subsistirá aun después de finalizada la relación con el responsable de la base de datos (art. 11).	NO.	NO.	NO.	NO.	NO.

	deberán ser eliminados aquellos datos que hayan caducado de acuerdo a lo previsto en la presente ley (art. 7).

Fuente y elaboración: La autora (2018).

De las tablas 27 y 28 se colige que existen los siguientes principios adicionales a los establecidos de manera general para la protección de datos personales:

- *Principio de licitud:* Argentina y Uruguay establecen que la formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos los datos personales, observando en su operación los principios que establece la presente ley y reglamento pertinente. Esta licitud también se verifica al establecer la obligación de que los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública. Uruguay añade además que las bases de datos no pueden tener finalidades violatorias de derechos humanos. México y Perú, por su parte, señalan que en el principio de licitud los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta ley y demás normatividad aplicable. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos o ilícitos. Panamá señala que el tratamiento de un dato personal sea lícito, deberá ser recolectado y tratado con el consentimiento previo, informado e inequívoco del titular del dato o por fundamento legal.
- *Principio de utilización no abusiva:* Los datos personales no podrán ser tratados con finalidades distintas o incompatibles con aquellas que motivaron su obtención.
- *Principio de cesión:* Argentina, no solo se reconoce como excepción al consentimiento sino como principio, señalando que los datos personales objeto de tratamiento solo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.
- *Principio de integridad:* Por el cual, se prohíbe que el manejo de los datos fuese incompleto, dado que esta situación puede distorsionar la veracidad de la información tal como señala Colombia. La Corte decidió tutelar los derechos de un usuario del sistema financiero que había sido afectado con una información incompleta. Por lo tanto, se ordenó a la entidad administradora de datos, completar la información acerca del comportamiento comercial del actor.
- *Principio de responsabilidad y rendición de cuentas:* Por el cual, el responsable debe elaborar y revisar periódicamente políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable y asignar recursos para su ejecución, así como servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología; poner en práctica un programa de capacitación y actualización; establecer un sistema de supervisión y

vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales; establecer procedimientos para recibir y responder dudas y quejas de los titulares, norma contenida en la legislación mexicana. Sin un texto que lo explique, Uruguay es otro de los países que contempla la responsabilidad como principio, pero de su lectura parece referirse a la responsabilidad, civil, administrativa y penal del responsable del tratamiento.

Para Brasil el principio de responsabilidad y rendición de cuentas hace alusión a la demostración de medidas efectivas de cumplimiento de las normas de protección de datos personales.

- *Principio de acceso y circulación restringida:* Colombia señala que el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados conforme a la presente ley. Brasil reconoce el principio de libre acceso por el cual el titular tiene derecho a un fácil acceso a la información sobre el procesamiento de sus datos, disponible de manera clara, apropiada y abierta.
- *Principio de proporcionalidad:* Perú reconoce que todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados. Panamá señala que solo deberán ser solicitados aquellos datos adecuados, pertinentes y limitados al mínimo necesario en relación con la finalidad para la que son requeridos.
- *Principio de necesidad: Brasil considera que este principio consiste* en la limitación del tratamiento al mínimo necesario para el cumplimiento de sus propósitos, relevantes, proporcionales y no excesivos en relación con los propósitos.
- *Principio de disposición:* Perú reconoce que todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.
- *Principio de nivel de protección adecuado:* Mediante el cual se garantiza un nivel suficiente de protección para los datos personales que se vayan a tratar fuera del país, por lo menos, equiparable a lo previsto por esta ley o por los estándares internacionales en la materia, conforme la normativa peruana.
- *Principio de lealtad:* Incluido generalmente en el principio de licitud, República Dominicana le da independencia cuando señala que se prohíbe recoger los datos por medios fraudulentos, desleales o ilícitos. Panamá señala que los datos personales deberán recabarse sin engaño o falsedad y sin utilizar medios fraudulentos, desleales o ilícitos.
- *Principio de veracidad:* Similar al anterior, denominado de esta manera en la legislación de Uruguay, pero que tiene por finalidad que la recolección de datos no pueda hacerse por medios desleales, fraudulentos, abusivos, extorsivos. Asimismo, aparece denominado como principio de veracidad, que señala que deberán tratarse datos veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. En consecuencia, los datos deberán ser exactos y es de cargo del responsable actualizarlos de ser necesario; si ha constatado la inexactitud o falsedad de los datos, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados, es decir, su contenido se asimila al principio de calidad reconocido generalmente.

- *Principio de reserva:* Se conoce en otra normativa como derecho de confidencialidad.
- *Principio de portabilidad:* Panamá reconoce este principio como aquel por el cual el titular de los datos tiene derecho a que el responsable del tratamiento le entregue una copia de sus datos personales en formato estructurada de uso común.
- *Principio de acceso gratuito:* Brasil considera que los titulares pueden consultar gratuita y fácil sobre la forma y duración del tratamiento, así como la integridad de sus datos personales.
- *Principio de no discriminación:* Brasil señala que no se debe permitir un tratamiento de datos personales con fines discriminatorios ilícitos o abusivos.
- *Principio de prevención:* Por el cual Brasil señala que es necesaria la adopción de medidas preventivas para evitar daños debido al procesamiento de datos personales.

Estos otros principios reconocidos por normativas latinoamericanas ayudan a la protección del derecho, por lo que aunque su incorporación no es parte del contenido esencial, es indispensable su análisis para verificar su necesidad de incorporarlo en las normativas de la región sobre todo porque se presentan para resolver necesidades propias de nuestras realidades sociales; así como resultado de los avances tecnológicos, en especial el principio de licitud y lealtad que ha sido incluido en casi todas las legislaciones analizadas.

1.5.5 Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

1.5.5.1 Derecho de acceso

Desde esta perspectiva, se colige lo siguiente:

Tabla 29

País	**Derecho de acceso**	***Habeas data* o procedimientos adecuados**	**Requiere trasgresiones a derechos para que prospere**
El Salvador	El artículo 31 de la Ley 534-2011 señala que toda persona, directamente o por intermedio de su representante, tendrá derecho a conseguir una reproducción inteligible de ella sin demora, anotándose que el acceso a los datos personales es exclusivo de su titular o su representante.	El artículo 32 determina que los entes obligados serán responsables de proteger los datos personales y, en relación con estos, deberán: a. Adoptar procedimientos adecuados para recibir y responder las solicitudes de indagatoria, actualización, modificación y supresión de datos personales. Es decir, por medio de los artículos 31 y 32 se determina condiciones para el ejercicio de una versión limitada de derecho de acceso al mencionar la obligación de las entidades de establecer procedimientos adecuados para solicitar y para entregar información a través de reproducciones inteligibles y sin demora.	NO.
Bolivia	NO.	En la Constitución de 2009, el artículo 130 determina descrita solo de forma negativa el derecho de acceso, rectificación y eliminación, pues solo cuando los responsables de los ficheros impidan de forma ilegal o indebida estos derechos es posible que opere la acción de protección de la privacidad.	También pueden eliminarse, rectificarse o accederse a datos siempre y cuando afecten los derechos fundamentales a la intimidad, privacidad, honra, propia imagen y buena reputación. Es decir, se requiere de presupuestos de ilegalidad y arbitrariedad para que la acción constitucional prospere. El sistema de protección no se basa ni en la titularidad del dato, ni en su consentimiento.
Chile	Aunque no consta descrito el derecho de acceso, en el artículo 13 de la Ley 19628 consta que el derecho de las personas a la información no puede ser limitado por medio de ningún acto o convención. En el mismo sentido, el artículo 14 determina que si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos.	NO.	NO.

Honduras	NO.	Únicamente se encuentra reconocido el derecho de acceso dentro de la garantía constitucional del *habeas data*, conforme el artículo 182 de la Constitución de Honduras.	Acceso solo a datos que produzcan daño al honor, la intimidad personal. En tal sentido, la norma establece que se activará esta garantía con la finalidad de obtener acceso a la información; es decir, a datos personales o familiares respecto de cualquier archivo o registro, privado o público.
Paraguay	El artículo 135 de la Constitución del Paraguay señala que toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público.	NO.	Conforme señala la jurisprudencia paraguaya este acceso se relaciona directamente al derecho a la intimidad en su relación con el derecho a la información
Venezuela	El artículo 28 de la Constitución señala que toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley.	NO.	NO.

Fuente y elaboración: La autora (2018).

De lo señalado en la tabla 29, se colige que el acceso como derecho está reconocido en El Salvador, Chile, Paraguay y Venezuela. El Salvador, aun cuando en este caso se refiere al derecho a conseguir una reproducción inteligible. En Chile no consta expresamente sino que en el artículo 14 de la Ley 19628 determina que si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos. Asimismo, la Constitución chilena con la reforma producida el 16 de junio de 2018 incluye el derecho a la protección de datos personales, pero no señala qué elementos lo constituyen. Por su parte, Paraguay y Venezuela determinan en sus respectivas Constituciones que toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público.

La novedad de la legitimación la establece la normativa venezolana, que establece que podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas.

El acceso reconocido como parte de la garantía de *habeas data* solo se reconoce en Honduras. Mientras que El Salvador determina establecer procedimientos adecuados para solicitar y para entregar información mediante reproducciones inteligibles y sin demora; y Bolivia la acción de protección de la privacidad.

Finalmente, Paraguay, Honduras y Bolivia señalan que para que prosperen las acciones pertinentes se requiere de trasgresiones a derechos como la intimidad, privacidad, entre otros.

c) Respecto del derecho a la protección de datos personales

Tabla 30

País	Derecho de acceso	Legitimado	Bancos de datos	Tratamiento	Gratuito	Reporte continuo	Procedimiento
Argentina	"ARTICULO 1. La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional".	El titular de los datos, previa acreditación de su identidad	El artículo 14 LPDP señala que el titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.	NO.	NO.	NO.	NO.
Brasil	El derecho de acceso se materializa mediante el habeas data contenido en el artículo 5 de la Constitución brasileña que permite el conocimiento de informaciones relativas a la persona que constan en registros o bancos de datos de entidades gubernamentales o de carácter público. Artículo 9 LGPD: El titular tiene derecho a un fácil acceso a la información sobre el procesamiento de sus datos, que debe estar disponible de manera clara, apropiada y abierta (...)"	El titular de los datos personales	El artículo 5 de la Constitución menciona en registros o bancos de datos	SI, procesamiento	SI, Art 6 LGPD "(...) IV - acceso gratuito: garantía a los titulares, consulta gratuita y fácil sobre la forma y duración del tratamiento, así como la integridad de sus datos personales; (...)"	NO	NO
Colombia	Art. 8 f. Ley 1581-2012. El titular de los datos personales tendrá los siguientes derechos: [...] f. Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.	Titular de los datos personales.	NO.	Tratamiento.	Gratuito.	NO.	NO.
Costa Rica	El artículo 7.1 de la Ley 8968 afirma que se garantiza el derecho de toda persona al acceso de sus datos personales, rectificación o supresión de estos y a consentir la cesión de sus datos.	Toda persona.	NO.	NO.	NO.	Asimismo, el derecho de acceso garantiza las facultades del interesado como: obtener en intervalos razonables la confirmación o no de la existencia de datos personales en archivos o bases de datos, y en caso de existencia sean comunicados en forma precisa y entendible.	NO.
Ecuador	Constitución de la República del Ecuador de 2008. Artículo 66, num.19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este	Toda persona, por sus propios derechos o como representante	Acceso a documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, sin costo alguno.	NO.	Sin costo alguno.	NO.	NO.

	carácter, así como su correspondiente protección. Artículo 92: Acceso sobre información y datos personales /	legitimado para el efecto (*habeas data*).					
Guatemala	ARTICULO 1. Objeto de la Ley. La presente ley tiene por objeto: [...] 2. Garantizar a toda persona individual el derecho a conocer y proteger los datos personales de lo que de ella conste en archivos estatales, así como de las actualizaciones de los mismos. Constitución de Guatemala de 1985, reformada en 1993.	A toda persona individual.	Derecho de acceso únicamente a ficheros públicos.	NO.	NO.	NO.	NO.
México	La Constitución mexicana, en el artículo 6, determina que toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de estos. De la misma manera, el artículo 16 menciona el derecho a la protección de datos personales cuando establece que toda persona tiene derecho al acceso, rectificación y cancelación de sus datos personales, así como a manifestar su oposición, en los términos que fije la ley. La LFPDPPP de 2010 determina que cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente ley.	Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización. Cualquier titular, o en su caso su representante legal.	Información pública y a sus datos personales o a la rectificación de éstos.	NO.	Acceso gratuito.	NO.	NO.
Nicaragua	El artículo 9 de la Ley de Protección de Datos Personales señala que el derecho de acceso se ejercerá mediante comunicación por escrito dirigida al responsable del fichero. El artículo 17 literal a) del mismo cuerpo legal señala que el titular de los datos personales tiene derecho solicitar y obtener información de sus datos personales tratados en los ficheros de datos públicos y privados.	Titular de los datos personales.	Ficheros de datos públicos y privados.	Tratados.	NO.	NO.	Mediante comunicación por escrito dirigida al responsable del fichero.
Panamá	Art. 42 y 44 de la Constitución panameña, relativo al *habeas data*, hacen mención expresa al derecho de toda persona a acceder a la información personal contenida en bases de datos o registros públicos y privados, con miras a garantizar el derecho de acceso a su información personal. El artículo 15 de la Ley 81 reconoce el derecho de acceso como aquel que "(...) permite al titular obtener sus datos personales que encuentren almacenados o sujetos a tratamiento en bases de datos de instituciones públicas o privadas, además de conocer el origen y la finalidad para los cuales han sido recabados".	Toda persona o el titular	Bases de datos o registros públicos y privados.	SI	SI, Art. 16 Ley 81 "(...) El suministro de información, la modificación, bloqueo o la eliminación de los datos personales será absolutamente gratuito y deberá proporcionarse, a solicitud del titular de los datos o quien lo represente, constancia de la base de datos actualizada en lo concerniente.	NO.	NO.
Perú	Por su parte, el artículo 19 de la Ley de Protección de Datos señala que el derecho de acceso permite al titular de datos personales el derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron	Titular de datos personales.	El derecho de acceso está presente en la Ley 28237, 31 de mayo de 2004. Código Procesal Constitucional en cuyo artículo 61 se indica que a través del proceso de *habeas data* se puede acceder a información que obre en poder de cualquier entidad pública, ya se trate de la que generen,	NO.	NO.	NO.	Asimismo, el artículo 63 respecto de la ejecución anticipada de oficio o a pedido de la parte reclamante, en cualquier etapa del procedimiento y antes de dictar sentencia, el juez está autorizado para requerir al demandado que posee, administra o maneja el archivo, registro o banco de datos, la

	recopilados, las razones que motivaron su recopilación y a solicitud de quien se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos.		produzcan, procesen o posean, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que la administración pública tenga en su poder, cualquiera que sea la forma de expresión, ya sea gráfica, sonora, visual, electromagnética o que obre en cualquier otro tipo de soporte material.				remisión de la información concerniente al reclamante; así como solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime conveniente. En este caso el derecho de acceso lo ejerce un titular a través de una acción específica de ejecución anticipada.
República Dominicana	El derecho de acceso se encuentra descrito en el artículo 44 de la Constitución de República Dominicana y es desarrollado por el artículo 10 de la Ley 172-13, por el cual se determina que el derecho de acceso, lo tiene toda persona, previa acreditación de su identidad, para acceder a la información y a los datos que sobre ella o sus bienes reposen en bancos de datos públicos, en los registros oficiales de las entidades, organismos y empresas públicas, así como sus datos registrados en los archivos de las instituciones y las empresas privadas, o en los bancos de datos privados. Por su parte, el artículo 8 de la citada ley señala las condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos, los datos personales de los que sea titular y que estén incluidos en un banco de datos. El artículo 9 de la citada ley señala la independencia de los derechos de acceso, rectificación, cancelación y oposición; es decir que estos son derechos independientes. No puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.	Toda persona, previa acreditación de su identidad.	Información y a los datos que sobre ella o sus bienes reposen en bancos de datos públicos, en los registros oficiales de las entidades, organismos y empresas públicas, así como sus datos registrados en los archivos de las instituciones y las empresas privadas, o en los bancos de datos privados.	NO.	NO.	NO.	El artículo 5, numeral 2, literal d), de la Ley 172-13 determina que los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular El usuario del banco de datos debe proporcionar la información solicitada por el titular de los datos dentro de cinco (5) días hábiles posteriores a haber sido hecha de manera personal dicha solicitud, o vía acto de alguacil. Vencido el plazo sin que se satisfaga el pedido, el titular de los datos podrá incoar una acción judicial ante un juzgado de primera instancia para conocer de la existencia y acceder a los datos que de él consten en registros o bancos de datos públicos o privados, conforme al procedimiento previsto en esta ley. Existe una confusión, pues el artículo 7 de la Ley 172-13 establece que el derecho de consulta para la protección de datos, por el cual toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de discriminación, inexactitud o error, exigir la suspensión, rectificación y la actualización de aquellos, conforme a esta ley. Esta acción judicial se refiere directamente al derecho de acceso.
Uruguay	La Ley 18.331 determina que todo titular de datos personales, debidamente identificado, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas. Este derecho de acceso solo podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico (art. 14).	Todo titular de datos personales, debidamente identificado.	Bases de datos públicas o privadas.	NO.	Ejercicio en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico (art. 14).	NO.	NO.

Fuente y elaboración: La autora (2018).

De la tabla 30, se concluye que Argentina, Colombia, Costa Rica, Ecuador, Guatemala, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay establecen uniformemente el derecho de acceso a la información o datos personales. Las variables en el contenido de este derecho se deben más bien a condiciones relativas al:

- *Legitimado:* Las normas analizadas establecen que el legitimado para interponer el derecho es toda persona, titular del dato personal. Pero en el caso de Argentina y República Dominicana se establece además que es necesaria la previa acreditación de la identidad de este. Asimismo, Ecuador y México establecen como legitimado al representante legal del titular. México además añade que podrán ser legitimados sin necesidad de acreditar interés alguno o justificar su utilización.
- *Bancos de datos:* En la redacción de este derecho se hace alusión a registros o bases de datos públicas y privadas. Ecuador y Perú, además, establecen otras formas de soporte como documentos, estudios, dictámenes, opiniones, datos estadísticos. Finalmente, Guatemala solo menciona este derecho exclusivamente para bases de datos públicas.
- *Tratamiento:* Brasil, Colombia, Panamá y Nicaragua hacen referencia a que el dato sea tratado para que proceda el derecho de acceso. El caso de Panamá el dato puede estar almacenado o tratado.
- *Gratuito:* Brasil, Ecuador, Colombia, Panamá y México establecen la gratuidad absoluta para el ejercicio del derecho de acceso. Uruguay establece un lapso de seis meses para esa gratuidad a menos que exista un interés legítimo.
- *Reporte continuo:* Costa Rica señala que dentro del derecho de acceso se garantiza obtener en intervalos razonables la confirmación o no de la existencia de datos personales en archivos o bases de datos y en caso de existencia sean comunicados en forma precisa y entendible.
- *Procedimiento:* Respecto de la forma en la que se puede solicitar el acceso, Nicaragua establece que debe hacerse mediante comunicación por escrito dirigida al responsable del fichero. Perú, por su parte, señala que en cualquier etapa del procedimiento y antes de dictar sentencia, el juez está autorizado para requerir al demandado que posee, administra o maneja el archivo, registro o banco de datos, la remisión de la información concerniente al reclamante. República Dominicana señala que los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso, dentro de cinco (5) días hábiles posteriores a la solicitud.

1.5.5.2 Derecho de rectificación

Desde esta perspectiva, se colige lo siguiente:

Tabla 31

País	Rectificación	Rectificar o completar los datos personales que fueren inexactos o incompletos	Requiere daño
El Salvador	El artículo 32 determina que los entes obligados serán responsables de proteger los datos personales y, en relación con éstos, deberán: a) Adoptar procedimientos adecuados para recibir y responder las solicitudes de indagatoria, actualización, modificación y supresión de datos personales y; d) Rectificar o completar los datos personales que fueren inexactos o incompletos.	Art. 32. "d) Rectificar o completar los datos personales que fueren inexactos o incompletos".	NO.
Bolivia	Según el artículo 130 de la Constitución boliviana "I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad".	NO.	La rectificación solo prospera cuando de forma ilegal o indebida el responsable del fichero se niegue a rectificar la información o esta afecta derechos fundamentales.
Chile	El literal j) del artículo 2 de la Ley 19628 determina que se entiende como modificación de datos, todo cambio en el contenido de los datos almacenados en registros o bancos de datos.	Derecho de rectificación a que en caso acreditarse que los datos personales sean erróneos, inexactos, equívocos o incompletos deban ser modificados, de forma gratuita	NO.
Honduras	El artículo 182 de la Constitución hondureña señala que el *habeas data* tiene la finalidad de rectificar datos inexactos o erróneos; actualizar información respecto de cualquier archivo o registro, privado o público, que conste en medios convencionales, electrónicos o informáticos, que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen.	El *habeas data* tiene la finalidad de rectificar datos inexactos o erróneos.	Rectificación solo de datos que produzcan daño al honor, la intimidad personal.
Paraguay	Según el artículo 135, del *habeas data*, "Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos".	Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.	Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.
Venezuela	La Constitución venezolana en el artículo 28 señala que toda persona podrá solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos datos personales que fuesen erróneos o afectasen ilegítimamente los derechos de sus titulares.	Rectificación o la destrucción de aquellos datos personales que fuesen erróneos	Solo de aquellos datos erróneos o que afecten ilegítimamente los derechos de los titulares.

Fuente y elaboración: La autora (2018).

De la tabla 31 se concluye que todos los países analizados reconocen el derecho de rectificación; la diferencia radica en las condiciones para su aplicabilidad, esto es que procede únicamente cuando los datos son erróneos (Venezuela y Paraguay), además inexactos (Chile, Honduras y El Salvador) o incompletos (El Salvador y Chile) e inequívocos (Chile).

Otra de las condiciones que debe producirse simultánea o individualmente es el daño. Así, en el caso de Bolivia requiere presupuestos de ilegalidad y arbitrariedad para que la acción constitucional prospere. Venezuela, Paraguay, Bolivia y Honduras requieren producir un daño a derechos fundamentales, principalmente al honor, la intimidad, la privacidad dependiendo del reconocimiento de cada uno de ellos en estos países.

Estos requisitos revelan un sistema de protección de los datos personales atado a la intimidad.

a) Respecto del derecho a la protección de datos personales

Tabla 32

País	Derecho de rectificación	Error o falsedad	Incompletos, inexactos	Afecten derechos	Tratamiento expresamente prohibido o no autorizado	Necesarios o pertinentes	Vencido el plazo para su tratamiento	Constancia de revisión	Gratuito	Negativa motivada a rectificación	Rectificación de medio de comunicación	Procedimiento secreto, judicial o administrativo o especial	Cesión, o información sobre la corrección a los responsables con los que se ha compartido datos
Argentina	Art. 16, LPDP. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. 2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.	Art. 16, LPDP 6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate.	Art. 19, LPDP. La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.	NO.	NO.	NO.	NO.	Art. 16, LPDP 6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.	Art. 19, LPDP. La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.	Art. 17, LPDP "1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros. 2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones	NO.	NO.	NO

										administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado. 3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa".				
Brasil	En el artículo 5, LXXII de la Constitución de la República Federativa del Brasil de 1988, se determina que se concederá *habeas data* a brasileños y extranjeros residentes en el país para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo. Art. 18. LGPD El titular de los datos personales tiene derecho a obtener del controlador, en relación con los datos del titular por él tratados, en cualquier momento y	NO	Art. 18. LGPD El titular de los datos personales tiene derecho a obtener del controlador, en relación con los datos del titular por él tratados, en cualquier momento y mediante solicitud: acápite acápite III - corrección de datos incompletos, inexactos u obsoletos; (…)"	NO.	NO.	NO.	NO.	NO.	SI, Art. 18, párrafo 5. LGPD. "(…) La solicitud a que se refiere el párrafo 3 de este artículo se atenderá sin costo alguno para el titular, dentro de los plazos y en los términos previstos en el reglamento.	SI, Art. 18 numeral II LGPD "(…)- indique las razones de hecho o de derecho que impiden la adopción inmediata de la medida.	NO.	Llama la atención que la norma establezca otra vía, esto es la de iniciar procedimiento secreto, judicial o administrativo (Art. 5 Constitución).	SI, Art. 18 Párrafo 6 LGPD "(…) La persona responsable informará inmediatamente a los agentes de tratamiento con los que ha hecho uso compartido de los datos sobre la corrección, eliminación, anonimato o bloqueo de los datos, para que repitan el mismo procedimiento, excepto en los casos en que esto la comunicación se demuestra imposible o conlleva un esfuerzo desproporcionado.

	mediante solicitud: acápite III - corrección de datos incompletos, inexactos u obsoletos; (…)”												
Colombia	El artículo 8 de la Ley 1581 señala entre los derechos de los titulares de los datos: a) Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.	Que induzcan a error. Artículo 17, Deberes de los responsables del tratamiento […], Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.	Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error.	NO.	Aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Costa Rica	Art. 7, Ley 8968. 1. Derechos que le asisten a la persona. Se garantiza el derecho de toda persona al acceso de sus datos personales, rectificación o supresión de estos y a consentir la cesión de sus datos. […] 2.2.- Todo titular puede solicitar y obtener de la persona responsable de la base de datos, la rectificación, la actualización, la cancelación o la eliminación y el cumplimiento de la	NO.	Art. 7, Ley 8968. Derecho de rectificación. Se garantiza el derecho de obtener, llegado el caso, la rectificación de los datos personales y su actualización o la eliminación de estos cuando se hayan tratado con infracción a las disposiciones de la presente ley, en particular a causa del carácter incompleto o inexacto de los	NO.	Hayan sido recolectados sin previo consentimiento de su titular o los mismos.	NO.	NO.	NO.	Art. 7, Ley 8968. “La persona responsable de la base de datos debe cumplir lo solicitado por la persona, de manera gratuita, y resolver en el sentido que corresponda en el plazo de cinco días hábiles, contado a partir de la recepción de la solicitud”.	NO.	NO.	NO.	NO.

	garantía de confidencialidad respecto de sus datos personales. El ejercicio del derecho al cual se refiere este artículo, en el caso de datos de personas fallecidas, les corresponderá a sus sucesores o herederos.		datos, o hayan sido recopilados sin autorización del titular.										
Ecuador	"La persona titular de los datos podrá solicitar al responsable [...] su rectificación". Art. 92, Constitución de la República del Ecuador, Registro Oficial 449, 20 de octubre de 2008.	Art. 50, Ley Orgánica de Garantías y Control Constitucional. "Ámbito de protección.- Se podrá interponer la acción de hábeas data en los siguientes casos: Cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos."	NO.	Art. 50, Ley Orgánica de Garantías y Control Constitucional. "Procede rectificación cuando los datos fueren erróneos o afecten sus derechos."	NO.	NO.	NO.	NO.	Art. 92, Constitución. "sin costo".	NO.	Art. 49, Ley Orgánica de Garantías y Control Constitucional. "Las presentes disposiciones son aplicables a los casos de rectificación a que están obligados los medios de comunicación, de conformidad con la Constitución. Deberá efectuarse una rectificación, réplica o respuesta, en forma inmediata, obligatoria y gratuita, en el mismo espacio u horario en el que se transmitió la información que causó el perjuicio".	NO.	NO.
Guatemala	"Art. 30. Hábeas data. Los sujetos	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	"Artículo 34.- Tratamiento de los	NO.	NO.	NO.

	obligados serán responsables de los datos personales y, en relación con éstos, deberán: 1. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos que sean, presentados por los titulares de los mismos o sus representantes legales, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos".									datos personales. Los titulares o sus representantes legales podrán solicitar, previa acreditación, que modifiquen sus datos personales contenidos en cualquier sistema de información. Con tal propósito, el interesado debe entregar una solicitud de modificaciones, en la que señale el sistema de datos personales, indique las modificaciones que desea realizar y aporte la documentación que motive su petición. El sujeto obligado debe entregar al solicitante, en un plazo no mayor de treinta días hábiles desde la presentación de la solicitud, una resolución que haga constar las modificaciones o bien, le informe de manera fundamentada, las razones por las cuales no procedieron las mismas".			
México	La Constitución mexicana, en el artículo 16 señala que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la	NO.	Art. 24, LPDPP. El titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos Art. 45, LPDPSO. El titular tendrá derecho a	NO.	NO.	NO.	NO.	NO.	Art. 50, LPDPSO. El ejercicio de los derechos ARCO deberá ser gratuito.	Art. 34, LPDPP. "El responsable podrá negar el acceso a los datos personales, o a realizar la rectificación o cancelación o conceder la oposición al tratamiento de los mismos, en los siguientes supuestos: I.	NO.	NO.	NO.

ley.

Entre tanto, la LFPDPPP de 2010 estipula que cualquier persona o su representante legal podrá ejercer los derechos de acceso, rectificación, cancelación y oposición (art. 22).

solicitar al responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.

Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello; II. Cuando en su base de datos, no se encuentren los datos personales del solicitante; III. Cuando se lesionen los derechos de un tercero; IV. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y V. Cuando la rectificación, cancelación u oposición haya sido previamente realizada. La negativa a que se refiere este artículo podrá ser parcial en cuyo caso el responsable efectuará el acceso, rectificación, cancelación u oposición requerida por el titular. En todos los casos anteriores, el responsable deberá informar el motivo de su decisión y comunicarla al titular, o en su caso, al representante legal, en los plazos establecidos para tal efecto, por el mismo medio por el que se llevó a cabo

									la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes".				
Nicaragua	Art. 19, Ley 787. Derechos de modificación de los datos. Toda persona tiene derecho a: "Solicitar la rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales de los que sea titular, que estén incluidos en un fichero de datos".	Art. 48, Ley 787. "La acción de protección de datos personales, procede: [...] c. En los casos en que se presuma la falsedad, inexactitud, desactualización, omisión, total o parcial, o ilicitud de la información de que se trata, para exigir su rectificación, actualización, modificación, inclusión, supresión o cancelación".	Art. 7, Ley 787, Ley h. "Los datos inexactos, incompletos, o que estén en desacuerdo con la realidad de los que le corresponden a la persona, serán rectificados, modificados, suprimidos, completados, incluidos, actualizados o cancelados según corresponda".	NO.	NO.	NO.	NO.	NO.	Art. 21. Gratuidad de modificación de los datos. "La rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales inexactos o incompletos que se encuentren en ficheros de datos se llevará a cabo de manera gratuita para el titular".	Art. 20, Ley 787. "Excepcionalidad para la modificación de los datos. Los responsables de ficheros de datos, pueden negar la rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales solicitada, cuando exista una resolución judicial que determine la no modificación".	NO.	NO.	NO.
Panamá	Art. 42, Constitución panameña. "Toda persona tiene derecho a acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley". El artículo 44 señala: "Mediante la acción de hábeas data se podrá solicitar que se corrija, actualice, rectifique, suprima o se mantenga en confidencialidad la información o datos que tengan carácter	El numeral 2 del artículo 15 de la Ley 81 señala que el derecho de rectificación "(...) permite al titular solicitar la corrección de sus datos personales que sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes".	Art. 17 de la Ley 81 señala que los datos "deberán ser modificados cuando sean erróneos, inexactos, equívocos o incompletos..." SI, Art. 16 Ley 81, "(...) y deberá proporcionarse, a solicitud del titular de los datos o quien lo represente, constancia de la base de datos actualizada en lo concerniente (...) Art. 17 Ley 81 "(...) En todo	NO.	SI, Art. 17 Ley 81 "(...) En todo caso, corresponderá a la Autoridad Nacional de Transparencia y Acceso a la Información, como autoridad competente, determinar cuándo un dato es inexacto o cuándo carece de fundamento legal, sin perjuicio de lo dispuesto en leyes especiales que regulen materias específicas	SI, Impertinentes.	NO.	NO.	SI, Art. 16 Ley 81, "(...) El suministro de información, la modificación, bloqueo o la eliminación de los datos personales será absolutamente gratuito (...)	NO.	NO.	SI; Art. 17 Ley 81 "(...). Los datos deberán ser modificados (...) dentro de un término de cinco días hábiles siguientes a la solicitud, de modificación, quien sea responsable de una base de datos regulada por esta Ley, podrá proceder a la eliminación, modificación o bloqueo de los datos personales sin necesidad de requerimientos del titular, cuando existan pruebas de inexactitud no	NO.

	personal". El numeral 2 del artículo 15 de la Ley 81 señala que el derecho de rectificación "permite al titular solicitar la corrección de sus datos personales que sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes".		caso, corresponderá a la Autoridad Nacional de Transparencia y Acceso a la Información, como autoridad competente, determinar cuándo un dato es inexacto o cuándo carece de fundamento legal, sin perjuicio de lo dispuesto en leyes especiales que regulen materias específicas"								pueda ser establecida o cuya vigencia y respecto de los cuales no corresponda la cancelación. En este caso, serán bloqueados para acceso a terceros o para evitar su uso en otros fines que no hayan sido los expresamente autorizados.	
Perú	El derecho de rectificación se lo encuentra en el numeral 2 del artículo 61 de Código Procesal Constitucional de 2004 cuando señala que el titular del dato podrá conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros.	El artículo 20 de la LPDP señala el derecho del titular de solicitar la actualización, inclusión, rectificación y supresión de sus datos personales, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad.	El artículo 20 de la LPDP señala el derecho del titular de solicitar la actualización, inclusión, rectificación y supresión de sus datos personales, cuando estos sean parcial o totalmente inexactos, incompletos.	NO.	NO.	Art. 20, LPDP. "[…] cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento".	Art. 20, LPDP. "[…] cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento".	NO.	NO.	NO.	NO.	NO.	NO.
República Dominicana	Art. 44, Ley 172-13, "Derecho a la intimidad y el honor personal. […] 2) Toda persona tiene el derecho a acceder	Art. 7, Ley 172-13, Derecho de consulta para la protección de datos. "Toda persona tiene	Art. 8, Ley 172-13. La rectificación, actualización o supresión de datos personales	NO.	NO.	NO.	NO.	NO.	Art. 8, Ley 172-13. "La rectificación, actualización o supresión de datos personales	El artículo 26 señala las excepciones a los derechos de acceso, rectificación, cancelación y	NO.	NO.	NO.

	a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. [...] Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos". El artículo 14 de la Ley 172-13 determina que toda persona tiene derecho a que sean rectificados, actualizados, y, cuando corresponda, suprimidos, los datos personales de los que sea titular y que estén incluidos en un banco de datos.	derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de discriminación, inexactitud o error, exigir la suspensión, rectificación y la actualización de aquellos, conforme a esta ley".	inexactos o incompletos que existan en registros públicos o privados					inexactos o incompletos que existan en registros públicos o privados se efectuará sin cargo alguno para el interesado".	oposición, cuando mediante resolución judicial los responsables o usuarios de bancos de datos oficiales pueden denegar el acceso, rectificación o la supresión en función de la protección de la seguridad nacional, del orden y la seguridad pública, o de la protección de los derechos e intereses de terceros, o cuando se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de crímenes y delitos por la autoridad competente y la verificación de infracciones administrativas.			
Uruguay	Art. 15, Ley 18.331. "Derecho de rectificación, actualización, inclusión o supresión.- Toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización, inclusión o supresión de los	Art. 15, Ley 18.331. "[...] al constatarse error o falsedad o exclusión en la información de la que es titular".	Artículo 10° del Decreto 414/099. "[...] la inexactitud o la incompletitud".	NO.	NO.	NO.	NO.	Durante el proceso de verificación, rectificación o inclusión de datos personales, ante el requerimiento de terceros por acceder a informes, deberá dejar	Art. 15, Ley 18.331. "La rectificación, actualización, inclusión, eliminación o supresión de datos personales cuando corresponda, se efectuará sin cargo alguno para	Art. 26. "Excepciones a los derechos de acceso, rectificación y cancelación.- Los responsables de las bases de datos que contengan los datos a que se refieren los incisos segundo y tercero del artículo anterior podrán denegar el acceso,	NO.	NO.	NO.

datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular".		constancia que dicha información se encuentra sometida a revisión (art. 15).	el titular".
			la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando. Los responsables de las bases de datos de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el inciso anterior cuando el mismo obstaculice las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el titular del dato esté siendo objeto de actuaciones inspectivas".

Fuente y elaboración: La autora (2018).

Todos los países analizados en la tabla 32 reconocen el derecho de rectificación por el cual se puede modificar datos personales, siempre y cuando se cumplan con las condiciones siguientes:

- *Error o falsedad:* Argentina, Colombia, Ecuador, Nicaragua, Panamá, Perú, República Dominicana y Uruguay señalan que solo pueden rectificarse datos personales errados o falsos. Únicamente en el caso de República Dominicana también se considera las características de que los datos sean discriminatorios. Colombia y Panamá señala que los datos incompletos o inexactos inducen a error.
- *Incompletos, inexactos o desactualizados:* Argentina, Brasil Colombia, Costa Rica, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay requieren para que sea posible el derecho de rectificación que los datos sean inexactos, incompletos o desactualizados. Ahora bien, Nicaragua añade las categorías de parciales, desactualizados, con omisión, total o parcial o ilícitos.
- *Afecten derechos:* Únicamente Ecuador determina que pueden rectificarse datos personales cuando afecten los derechos del titular.
- *Tratamiento expresamente prohibido o no autorizado:* Costa Rica determina también como posible condición para rectificar datos personales, el que no hayan sido autorizados por sus titulares. En el mismo sentido lo establece Colombia, pero añade otra característica: que esté expresamente prohibida. Panamá por su parte señala que será a la autoridad de control la competente para determinar cuándo un dato carece de fundamento legal.
- *Necesarios o pertinentes:* Perú y Brasil determinan que pueden rectificarse datos que ya no sean pertinentes, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados.
- *Vencido el plazo para su tratamiento*: Perú señala que pueden ser rectificados cuando se hubiera vencido el plazo establecido para su tratamiento.
- *Constancia de revisión:* Argentina y Uruguay establecen que durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá: o bien bloquear el archivo o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión. Esta advertencia es útil para quien va a seguir utilizando o ha dejado de utilizar el dato y aún no existe motivación de su rectificación.

Finalmente, respecto del derecho de rectificaciones varias legislaciones establecen variantes para su adecuada ejecución que se analizarán a continuación.

- *Gratuito:* Argentina, Brasil Costa Rica, Ecuador, México, Nicaragua, Panamá, República Dominicana y Uruguay determinan que la rectificación del dato personal no tendrá costo para el titular.
- *Negativa motivada a rectificación:* Argentina, Brasil, Guatemala, México, Nicaragua, República Dominicana y Uruguay establecen excepciones por las cuales los derechos de acceso, rectificación y cancelación, en este caso el que nos interesa el de rectificación, no deberán prosperar; es decir, no permiten modificar datos personales en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

En el caso de República Dominicana y Argentina señalan como excepciones, además, cuando se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de crímenes y delitos por la autoridad competente y la verificación de infracciones administrativas.

Nicaragua y Argentina autorizan la negativa cuando exista una resolución judicial que lo determine.

Argentina, por su parte, establece también excepciones formales: si el solicitante no es titular de los datos personales, o el representante legal no esté debidamente acreditado, no se encuentren los datos personales del solicitante en la base de datos, cuando haya sido previamente realizada.

Asimismo, Uruguay y República Dominicana señalan que los responsables de las bases de datos de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el inciso anterior cuando el mismo obstaculice las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias.

Uruguay, Guatemala y Argentina, además, establecen que ante la negativa los titulares tienen derecho a solicitar una revisión de la negativa ante autoridad competente.

Panamá señala que, se puede realizar rectificación de oficio es decir sin que medie requerimientos del titular, cuando existe pruebas de inexactitud no pueda ser establecida o cuya vigencia y respecto de los cuales no corresponda la cancelación.

- *Rectificación de medio de comunicación:* Únicamente Ecuador confunde la rectificación en medios de comunicación con el derecho de rectificar datos personales en bases o registros públicos o privados, cuando se desprenden de situaciones fácticas completamente diferentes y su naturaleza proviene de distintos derechos fundamentales, el primero relacionado al derecho a la libertad de expresión y, el segundo, al derecho a la protección de datos personales, específicamente al derecho de autodeterminación informativa.

- *Cesión o información sobre la corrección a los responsables con los que se ha compartido datos: Brasil,* establece la obligación de informar al responsable de tratamiento que recibió mediante mecanismo de uso compartido de datos de las modificaciones y la obligación de realizarlas.

  Finalmente, Brasil establece la posibilidad de otra vía distinta del *habeas data*: un procedimiento secreto, judicial o administrativo, menciona que el titular de los datos personales tiene derecho a obtener del controlador, en relación con los datos del titular por él tratados, en cualquier momento y mediante solicitud: la corrección de datos incompletos, inexactos o desactualizados.

1.5.5.3 Derecho de actualización

Desde esta perspectiva, se colige lo siguiente:

Tabla 33

País	Derecho de actualización
El Salvador	NO.
Bolivia	NO.
Chile	Refiriéndose a finalidad de los datos, el artículo 9° de la Ley 19628 determina que los datos personales deben ser exactos, actualizados y responder con veracidad a la situación real del titular de los datos.
Honduras	Art. 182. 1. Para obtener acceso a la información; impedir su transmisión o divulgación; rectificar datos inexactos o erróneos; actualizar información, exigir confidencialidad y la eliminación de información falsa; respecto de cualquier archivo o registro, privado o público, que conste en medios convencionales, electrónicos o informáticos, que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen. Esta garantía no afectará el secreto de las fuentes de información periodística.
Paraguay	El artículo 7° de la Ley 1682-2001 dice que serán actualizados permanentemente los datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales que, de acuerdo con esta ley, pueden difundirse o publicarse.
Venezuela	La Constitución venezolana, en el artículo 28, señala que toda persona podrá solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos datos personales que fuesen erróneos o afectasen ilegítimamente los derechos de sus titulares.

Fuente y elaboración: La autora (2018).

Según lo señalado en la tabla 33, solamente Chile, Honduras, Paraguay y Venezuela recogen el término actualización. En el caso de Chile constan, entre todos, los elementos que configuran el principio de calidad de datos. En Paraguay no consta como derecho sino como deber de actualización por parte del responsable de bases de datos de solvencia económica; esto debido a que el derecho-deber de actualización proviene de la utilizan de esta información para el giro de sus operaciones.

En Venezuela y Honduras se consideran aquellos datos erróneos o que afecten ilegítimamente los derechos de los titulares, en específico el derecho a la intimidad, por lo que el derecho de actualización tiene una limitación evidente.

a) Respecto del derecho a la protección de datos personales

Tabla 34

País	Derecho de actualización	Error o falsedad	Incompleto e inexacto	Afecten derechos	Sin consentimiento titular o prohibidos	Mantener actualizada	Titulares obligados a actualizar	Constancia de revisión	Gratuito	Negativa motivada a rectificación
Argentina	Art. 16, LPDP. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. 2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.	Art. 16, LPDP 6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate.	Art. 19, LPDP. La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.	NO.	NO.	NO.	NO.	Art. 16, LPDP 6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.	Art. 19, LPDP. La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.	NO. El artículo 17 no menciona la actualización sino únicamente la rectificación, aunque se entiende incluida en esta.
Brasil	Art. 6, acápite V LGPD – "(...) calidad de los datos: garantía a los propietarios, precisión, claridad, relevancia y actualización de los datos, de acuerdo con la necesidad y para el cumplimiento del propósito de su procesamiento;(...)" (principio de calidad de los datos) Art. 18. LGPD El titular de los datos personales tiene derecho a obtener del controlador, en relación con los datos del titular por él tratados, en cualquier momento y mediante solicitud: (...) acápite III - corrección de datos incompletos, inexactos u obsoletos;(...)" (derecho de rectificación)	NO	NO, El artículos 6 se refiere al principio de calidad del dato y el 18 de la LPDP no menciona la actualización como derecho sino únicamente a la rectificación, aunque se entiende incluida en esta.	NO.	NO.	Artículo 50. Los controladores y operadores, dentro del alcance de sus competencias, para el procesamiento de datos personales, individualmente o a través de asociaciones, pueden formular reglas de buenas prácticas y gobernanza que establezcan las condiciones de organización, el régimen operativo, el procedimientos, incluidas las quejas y peticiones de los titulares, normas de seguridad, normas técnicas, obligaciones específicas para las diversas partes involucradas en el procesamiento, acciones educativas, mecanismos internos de supervisión y	NO.	NO.	NO, El artículos 6 se refiere al principio de calidad del dato y el 18 de la LPDP no menciona la actualización como derecho sino únicamente a la rectificación, aunque se entiende incluida en esta.	SI, Art. 18 numeral II LGPD "(...)- indique las razones de hecho o de derecho que impiden la adopción inmediata de la medida.

						mitigación de riesgos y otros aspectos relacionados con el procesamiento de datos personal (...) h) se actualiza constantemente con base en la información obtenida del monitoreo continuo y evaluaciones periódicas				
Colombia	Artículo 1°, Ley 1581-2012. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. Entre tanto, el artículo 4, literal d), sobre el principio de veracidad o calidad afirma que "La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error".	Artículo 8°, Ley 1581-2012. Derechos de los Titulares. "El Titular de los datos personales tendrá los siguientes derechos: a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error".	Artículo 8°. Derechos de los Titulares. "El Titular de los datos personales tendrá los siguientes derechos: a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados".	NO.	Artículo 8°. Ley 1581-2012. Derechos de los Titulares. "El Titular de los datos personales tendrá los siguientes derechos: a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, [...] esté expresamente prohibido o no haya sido autorizado".	Artículo 17, Ley 1581-2012. Deberes de los Responsables del Tratamiento. "f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada".	NO.	NO.	NO.	NO.
Costa Rica	Según el artículo 7.2 de la ley 8968, se garantiza el derecho de rectificación, actualización o eliminación sobre datos personales o sobre la garantía de confidencialidad respecto a los mismos; en el primer caso a causa de carácter incompleto o inexacto o hayan sido recolectados sin previo consentimiento de su titular o los mismos.	Erróneos.	Incompleto o inexacto o hayan sido recolectados.	NO.	Sin previo consentimiento de su titular o los mismos.	NO.	NO.	NO.	Art. 7, Ley 8968. "La persona responsable de la base de datos debe cumplir lo solicitado por la persona, de manera gratuita, y resolver en el sentido que corresponda en el plazo de cinco días hábiles, contado a partir de la recepción de la solicitud".	NO.

Ecuador	Art. 92, Constitución de la República del Ecuador, Registro Oficial 449, 20 de octubre de 2008. "La persona titular de los datos podrá solicitar al responsable [...] la actualización de los datos. Procede actualización cuando los datos fueren erróneos o afecten sus derechos".	Art. 50, Ley Orgánica de Garantías y Control Constitucional. "Procede rectificación cuando los datos fueren erróneos o afecten sus derechos".	NO.	Art. 50, Ley Orgánica de Garantías y Control Constitucional. "Procede cuando los datos fueren erróneos o afecten sus derechos".	NO.	NO.	NO.	NO.	Art. 92. Constitución. Sin costo.	NO.
Guatemala	Art. 1, núm. 2. "Objeto de la Ley. La presente ley tiene por objeto: [...] 2. Garantizar a toda persona individual el derecho a conocer y proteger los datos personales de lo que de ella conste en archivos estatales, así como de las actualizaciones de los mismos".	NO.	NO.	NO.	NO.	Art. 30. "Hábeas data. Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán: [...] 4. Procurar que los datos personales sean exactos y actualizados".	Art. 7. Actualización de información. "Los sujetos obligados deberán actualizar su información en un plazo no mayor de treinta días, después de producirse un cambio".	NO.	NO.	El artículo 34 no menciona expresamente la actualización, pero se entiende dentro de la rectificación.
México	LGPDPPSO de 2017. Al igual que en el caso del derecho de acceso, la normativa determina que en todo momento el titular o su representante podrán solicitar el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen (art. 43). En el caso del derecho de rectificación, el titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados (art. 45). Solo en la ley aplicable al ámbito público consta dentro de las condiciones para solicitar la rectificación que los datos estén desactualizados.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Nicaragua	Art. 19, Ley 787. Derechos de modificación de los datos. "Toda persona tiene derecho a: a. A Solicitar la rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales de los que sea titular, que estén incluidos en un fichero de datos".	Art. 48, Ley 787. "La acción de protección de datos personales, procede: [...] c. En los casos en que se presuma la falsedad, inexactitud, desactualización, omisión, total o parcial, o ilicitud de la información de que se trata, para exigir su rectificación, actualización, modificación, inclusión,	Art. 7, Ley 787, Ley h. "Los datos inexactos, incompletos, o que estén en desacuerdo con la realidad de los que le corresponden a la persona, serán rectificados, modificados, suprimidos, completados, incluidos, actualizados o cancelados según	NO.	NO.	NO.	NO.	NO.	Art. 21. Gratuidad de modificación de los datos. "La rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales inexactos o incompletos que	Art. 20, Ley 787. Excepcionalidad para la modificación de los datos. Los responsables de ficheros de datos pueden negar la rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales solicitada, cuando exista una resolución judicial que determine la no modificación.

		supresión o cancelación".	corresponda".					se encuentren en ficheros de datos se llevará a cabo de manera gratuita para el titular".	
Panamá	Artículo 2 Ley 81.- "(…) 4. Principio de veracidad y exactitud: los datos de carácter personal serán exactos y puestos al día de manera que respondan con veracidad a la situación actual del propietario del dato.	NO.	SI. El Art. 4 numeral 8, Ley 81 menciona el término dato caduco que es "(…) Aquel dato que ha perdido actualidad por disposición de la Ley, por el cumplimiento de la condición o la expiración del plazo señalado para vigencia o, si no hubiera norma expresa, por el cambio de los hechos o circunstancia que consigna.	NO.	NO.	SI. El Art. 31, Ley 81 señala que los responsables y/o custodios de bases de datos que transfieran datos personales almacenados en bases de datos a terceros llevarán un registro de estas y deberán estar a disposición de la Autoridad Nacional de Transparencia y Acceso de la Información en caso de que esta lo requiera para cumplir con las facultades le otorga esta Ley. En el registro al que se refiere el párrafo anterior contará, respecto de cada una de esas bases de datos (…) los procedimientos a realizar para la rectificación, la actualización de los datos, el tiempo de conservación de los datos (…).	NO.	NO.	SI. Art. 16, Ley 81 El suministro de información, la modificación, bloqueo o la eliminación de los datos personales será absolutamente gratuito y deberá proporcionarse, a solicitud del titular de los datos o quien lo represente, constancia de la base de datos actualizada en lo concerniente.	NO.
Perú	El artículo 20 de la LPDP señala el derecho del titular de solicitar la actualización, inclusión, rectificación y	El artículo 20 de la LPDP señala el derecho del titular de solicitar la	El artículo 20 de la LPDP señala el derecho del titular de	El artículo 20 de la LPDP señala el derecho del titular de solicitar la	NO.	NO.	NO.	NO.	NO.	NO.

	supresión de sus datos personales; cuando estos sean parcial o totalmente inexactos, incompletos; cuando se hubiere advertido omisión, error o falsedad; cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento.	actualización, inclusión, rectificación y supresión de sus datos personales, cuando estos sean parcial o totalmente inexactos, incompletos; cuando se hubiere advertido omisión, error o falsedad.	solicitar la actualización, inclusión, rectificación y supresión de sus datos personales, cuando estos sean parcial o totalmente inexactos, incompletos.	actualización, inclusión, rectificación y supresión de sus datos personales, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopiladas o cuando hubiera vencido el plazo establecido para su tratamiento.					
República Dominicana	Art. 44, Ley 172-13. Derecho a la intimidad y el honor personal. "2) Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. [...] Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos. El artículo 14 de la Ley 172-13 determina que toda persona tiene derecho a que sean rectificados, actualizados, y, cuando corresponda, suprimidos, los datos personales de los que sea titular y que estén incluidos en un banco de datos.	Art. 7, Ley 172-13. Derecho de consulta para la protección de datos. Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de discriminación, inexactitud o error, exigir la suspensión, rectificación y la actualización de aquellos, conforme a esta ley.	Art. 8, Ley 172-13. La rectificación, actualización o supresión de datos personales inexactos o incompletos que existan en registros públicos o privados.	NO.	NO.	NO.	NO.	NO.	Art. 8, Ley 172-13. "La rectificación, actualización o supresión de datos personales inexactos o incompletos que existan en registros públicos o privados se efectuará sin cargo alguno para el interesado".	El artículo 26 no menciona expresamente actualización, pero se entiende incluido en la rectificación.
Uruguay	Art. 15, Ley 18.331. Derecho de rectificación, actualización, inclusión o supresión. "Toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular".	Según el artículo 15 de la Ley 18.331 "al constatarse error o falsedad o exclusión en la información de la que es titular".	Según el artículo 10° del Decreto 414/099 "la inexactitud o la incompletitud".	NO.	NO.	NO.	El Decreto 414/009 determina el derecho de actualización, por el cual el titular puede modificar los datos que resulten inexactos a la fecha de ejercicio del derecho (art. 11°). Este derecho permite materializar el principio de calidad de	Durante el proceso de verificación, rectificación o inclusión de datos personales, ante el requerimiento de terceros por acceder a informes, deberá dejar constancia que dicha información se encuentra sometida a revisión (art. 15).	Art. 15, Ley 18.331. "La rectificación, actualización, inclusión, eliminación o supresión de datos personales cuando corresponda, se efectuará sin cargo alguno para el titular".	No menciona la actualización de forma expresa en el artículo 26, pero se entiende incluido en la rectificación.

datos.

Fuente y elaboración: La autora (2018).

Según la tabla 34, todos los países han desarrollado el derecho de actualización de forma directa o indirecta, mediante el derecho de rectificación como lo hace México que lo tiene de forma clara para los ficheros públicos, pero de forma indirecta para ficheros privados, por ejemplo. Brasil lo hace además en el principio de calidad de datos y Panamá en el de veracidad y exactitud de datos. Ahora bien, han establecido requisitos para su procedibilidad:

- *Error o falsedad:* Solo podrán actualizarse datos que sean errados o falsos, conforme lo señala la normativa de Argentina, Ecuador, Colombia Costa Rica, México, Nicaragua, Perú, República Dominicana y Uruguay. Colombia indica que los datos incompletos o inexactos inducen a error.
- *Incompleto e inexacto:* La actualización únicamente opera si los datos son incompletos o inexactos según Argentina, Colombia, Costa Rica, Perú, República Dominicana y Uruguay. Ahora bien, Nicaragua añade las categorías de parciales, desactualizados, con omisión, total o parcial, o ilícitos. Panamá menciona el concepto de dato caduco que es aquel que se produce por el cambio de legislación, cumplimiento del plazo o cambio de circunstancias.
- *Afecten derechos:* Ecuador es el único que establece que prospera la actualización si se afectan derechos de los titulares.
- *Sin consentimiento del titular o prohibido por la ley:* Colombia, Costa Rica y Ecuador determinan que puede actualizarse información personal cuando esta haya sido obtenida sin consentimiento.
- *Mantener actualizada:* Brasil, Colombia, Panamá y Guatemala establecen la obligación del responsable del fichero o base de datos que la información se mantenga actualizada.
- *Titulares obligados a actualizar:* Asimismo, Guatemala y Uruguay establecen la obligación de que sean los propios titulares que, conociendo sus datos, reporten o actualicen su información personal.
- *Gratuidad:* Argentina, Brasil, Costa Rica, Ecuador, Nicaragua, Panamá, República Dominicana y Uruguay establecen que la actualización no tiene costo alguno para el titular. México no menciona expresamente actualización sino derechos ARCO.
- *Constancia de revisión:* Argentina y Uruguay señalan que mientras se suscita un cambio en la información, es decir se actualiza, debe constar que se está revisando la información para que no sea utilizada hasta que la decisión de su cambio se produzca.
- *Negativa motivada a rectificación:* Si bien, Argentina, Brasil, Guatemala, México, Nicaragua, República Dominicana y Uruguay establecen causales claras por las cuales se puede negar el responsable de una base de datos a modificar datos personales (véase rectificación); sin embargo, en ninguno de esos países consta expresa mención al derecho de actualización en la redacción de estas normas específicas, por lo que se entiende incorporado este derecho en el de rectificación.

1.5.5.4 Derecho de cancelación

Desde esta perspectiva, se colige lo siguiente:

Tabla 35

País	Supresión de datos: proceder	Datos erróneos o falsos	Daño a derechos fundamentales	Datos caducos
El Salvador	El artículo 32 de la Ley 534-2011 establece que los entes obligados serán responsables de proteger los datos personales y, en relación con estos, deberán adoptar procedimientos adecuados para recibir y responder las solicitudes de indagatoria, actualización, modificación y supresión de datos personales.	NO.	NO.	NO.
Bolivia	NO.	NO.	Consta descrita como derecho de eliminación asociado únicamente cuando el responsable de una base de datos se niega de forma ilegal o indebida a eliminar datos, sobre todo si su permanencia afectan derechos fundamentales (art. 130, Constitución boliviana de 2009).	NO.
Chile	NO.	NO.	NO.	Según el artículo 12 de la Ley 19628, sin perjuicio de las excepciones legales, podrá eliminarse (que consiste en la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello, (art. 2) o bloquearse datos personales (por el cual se suspende de forma temporal cualquier operación de tratamiento de datos almacenados, (art. 2) cuando su almacenamiento carezca de fundamento legal, estuvieren caducos, cuando si bien fueron proporcionados voluntariamente o se usen para comunicaciones comerciales y ya no se desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.
Honduras	NO.	"Para obtener acceso a la información; impedir su transmisión o divulgación; rectificar datos inexactos o erróneos; actualizar información, exigir confidencialidad y la eliminación de información falsa".	Art. 182, Constitución de la República de Honduras. "Para obtener acceso a la información; impedir su transmisión o divulgación; rectificar datos inexactos o erróneos; actualizar información, exigir confidencialidad y la eliminación de información falsa; respecto de cualquier archivo o registro, privado o público, que conste en medios convencionales, electrónicos o informáticos, que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen. Esta garantía no afectará el secreto de las fuentes de información periodística".	NO.
Paraguay	NO.	El artículo 135 de la Constitución del Paraguay establece la actualización, la rectificación o la destrucción de los datos. Los datos pueden destruirse únicamente cuando los datos son falsos y en contrario sentido, no podrán ser destruidos si los datos son comprobadamente	NO.	NO.

		exactos.		
Venezuela	NO.	La Constitución venezolana, en el artículo 28, señala que toda persona podrá solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos datos personales que fuesen erróneos.	La Constitución venezolana, en el artículo 28, señala que toda persona podrá solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquéllos datos personales que fuesen erróneos o afectasen ilegítimamente los derechos de sus titulares.	NO.

Fuente y elaboración: La autora (2018).

En estos países analizados en la tabla 35, se colige lo siguiente:

- *Supresión de datos:* Respecto de la supresión como derecho, no se distingue entre este y la cancelación. En el caso de El Salvador, se refiere directamente a la supresión o eliminación de datos.
- *Datos erróneos o falsos:* Honduras y Paraguay señalan que para que un dato sea eliminado la condición es que sea falso; solamente a Venezuela le basta que sea erróneo.
- *Daño a derechos fundamentales:* Asimismo, para que proceda la eliminación se requiere que el dato personal afecte derechos fundamentales como la intimidad, la privacidad, el honor, la imagen, entre otros, tal como señalan Bolivia, Honduras y Venezuela.
- *Datos caducos:* Chile, por su parte, señala que la condición necesaria para que un dato sea eliminado es que se encuentre caduco.

Como se evidencia, no existe uniformidad sobre qué motivos son los razonables para eliminar datos personales ni las justificaciones adecuadas que apuntalan el contenido de este derecho.

a) Respecto del derecho a la protección de datos personales:

Tabla 36

País	Supresión, eliminación o cancelación	Errados o falsos	Incompletos o inexactos	Innecesarios, impertinentes irrelevantes, desfasados, excesivos, tratados en violación a la ley o sin consentimiento	Afecte derechos o finalidad	No cumplen finalidad	Final del procesamiento	Plazo vencido	Gratuito	Negativa motivada a supresión	Obligación del responsable	Bloqueo	Cesión, o información sobre la corrección a los responsables con los que se ha compartido datos
Argentina	Art. 16, LPDP. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. [...] 2. El responsable o usuario del banco de datos debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.	Art. 16, LPDP 6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate	NO	NO.	NO.	NO.	NO.	NO.	Art. 19, LPDP. La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.	Art. 16.5, LPDP. Específicamente sobre la supresión, se aclara que esta no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos. Art. 17 LPDP 1. "[...] denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros. [...] cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas".	NO.	Art. 16, LPDP 6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.	Art. 16. 1, LPDP. "4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato".
Brasil	Artículo 5 XIV - eliminación: eliminación de datos o conjunto de datos almacenados en la base de datos, independientemente del procedimiento empleado; (...) Art. 18 acápite IV - anonimato, bloqueo o eliminación de datos innecesarios, excesivos o tratados en violación de las disposiciones de esta Ley; (...)"VI -	NO.	NO.	SI (...) Art. 18 acápite IV - anonimato, bloqueo o eliminación de datos innecesarios, excesivos o tratados en violación de las disposiciones de esta Ley; (...)"VI -	NO.	NO.	Art. 16. Los datos personales serán eliminados después del final de su procesamiento,	NO.	SI, Art. 18, párrafo 5. LGPD. "(...) La solicitud a que se refiere el párrafo 3 de este artículo se atenderá sin costo alguno para el titular,	SI, Art. 18 numeral II LGPD "(...)- indique las razones de hecho o de derecho que impiden la adopción inmediata de la medida.	NO.	SI, Art. 18 Párrafo 6., LGPD "(...)- La persona responsable informará inmediatamente a los agentes de tratamiento con los que ha hecho uso compartido de los datos sobre la corrección, eliminación, anonimato o bloqueo	SI, Art. 18 Párrafo 6 LGPD "(...) La persona responsable informará inmediatamente a los agentes de tratamiento con los que ha hecho uso compartido de los datos sobre la corrección, eliminación, anonimato o bloqueo de los datos, para que repitan el mismo procedimiento, excepto en

	eliminación de datos personales procesados con el consentimiento del titular, excepto en los casos previstos en el art. 16 de esta Ley; (…)"			eliminación de datos personales procesados con el consentimiento del titular, excepto en los casos previstos en el art. 16 de esta Ley; (…)"				dentro de los plazos y en los términos previstos en el reglamento.			de los datos, para que repitan el mismo procedimiento, excepto en los casos en que esto la comunicación se demuestra imposible o conlleva un esfuerzo desproporcionado.	los casos en que esto la comunicación se demuestra imposible o conlleva un esfuerzo desproporcionado.
Colombia	Art. 8, Ley 1581-2012. Derecho de los titulares. […] e) Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a esta ley y a la Constitución. Art. 9°, Decreto 1377 de 2013. Revocatoria de la autorización y/o supresión del dato. "Los Titulares podrán en todo momento solicitar al responsable o encargado la supresión de sus datos personales y/o revocar la autorización otorgada para el Tratamiento de los mismos, mediante la presentación de un reclamo, de acuerdo con lo establecido en el artículo 15 de la Ley 1581 de 2012".	NO.	NO.	NO.	Art. 8, Ley 1581-2012. Derecho de los titulares. "e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.	NO.	NO.	NO.	Art. 9°, Decreto 1377. "El responsable y el encargado deben poner a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada".	Art. 9°, Decreto 1377 de 2013. "La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos".	NO.	Art. 21, Ley 1581-2012. Funciones. "La Superintendencia de Industria y Comercio ejercerá las siguientes funciones: […] c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva".	NO.
Costa Rica	Art. 7, Ley 8968. Derechos que le asisten a la persona. Se garantiza el derecho de toda persona al acceso de sus datos personales, rectificación o supresión de estos y a consentir la cesión de sus datos. En este contexto, el artículo 25 desarrolla este derecho como la posibilidad del titular para solicitar la supresión o eliminación al responsable	NO.	NO.	NO.	NO.	Art. 23, LPDPSO. Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de	NO.	NO.	Art. 7, Ley 8968. La persona responsable de la base de datos debe cumplir lo solicitado por la persona, de manera gratuita, y resolver en el sentido	NO.	Art. 2, Decreto Ejecutivo 37554. En el artículo 2 se define supresión o eliminación como el procedimiento en el que el responsable borra o	Según el artículo 23, LPDPSO, "previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos".	

	conforme lo fundamentado en el artículo 2.				privacidad y que motivaron su tratamiento a las disposiciones que resulten aplicables, deberán ser suprimidas.			que corresponda en el plazo de cinco días hábiles, contado a partir de la recepción de la solicitud.		destruye total o parcialmente de manera definitivas, los datos personales de la base de datos del titular.		
Ecuador	"La persona titular de los datos podrá solicitar al responsable [...] la eliminación o anulación de los datos". Constitución de la República del Ecuador 2008. Art. 50, Ley Orgánica de Garantías y Control Constitucional. Ámbito de protección. "Se podrá interponer la acción de hábeas data en los siguientes casos: Cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten derechos".	Art. 50, LOGCC. "Datos fueren erróneos".	NO.	NO.	Art. 50, LOGCC, "afecten derechos".	NO.	NO.	NO.	Art. 92, Constitución. "sin costo".	Art. 49, LOGCC, Ley Orgánica de Garantías y Control Constitucional. "No podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos".	NO.	NO.	NO.
Guatemala	NO.									NO.			
México	El artículo 22, LFPDPPP de 2010, estipula que cualquier persona o su representante legal podrán ejercer los derechos de acceso, rectificación, cancelación y oposición. Según el artículo 25, LFDPPP, el titular tendrá en todo momento el derecho a cancelar sus datos personales. Art. 3, LOPDPSO. "Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente	NO.	NO.	NO.	NO.	NO.	NO.	NO.	Art. 50, LPDPSO. El ejercicio de los derechos ARCO deberá ser gratuito.	Según el artículo 34, LPDPP. "El responsable podrá negar el acceso a los datos personales, o a realizar la rectificación o cancelación o conceder la oposición al tratamiento de los mismos, en los siguientes supuestos: I. Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello; II. Cuando en su base de datos, no se encuentren los datos personales del solicitante; III. Cuando se lesionen los derechos de un tercero; IV. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y V. Cuando la	NO.	Según el artículo 25, LFPDPPP de 2010, "El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento. Una vez cancelado el dato se dará aviso a su titular. Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o	

	establecidas por el responsable".								rectificación, cancelación u oposición haya sido previamente realizada. La negativa a que se refiere este artículo podrá ser parcial en cuyo caso el responsable efectuará el acceso, rectificación, cancelación u oposición requerida por el titular. En todos los casos anteriores, el responsable deberá informar el motivo de su decisión y comunicarla al titular, o en su caso, al representante legal, en los plazos establecidos para tal efecto, por el mismo medio por el que se llevó a cabo la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes".	cancelación, para que proceda a efectuarla también". Según el artículo 3, LOPDPSO, "Bloqueo: Es la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda".	
Nicaragua	Art. 19, LPDP. Derechos de modificación de los datos. Toda persona tiene derecho a: "a. A Solicitar la rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales de los que sea titular, que estén incluidos en un fichero de datos".	NO.	NO.	NO.	Art. 19, LPDP. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad que dio lugar a su tratamiento.	NO.	NO.	NO.	Art. 21, Gratuidad de modificación de los datos. "La rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales inexactos o incompletos que se encuentren en ficheros de datos se	Art. 19, LPDP. "La cancelación de los datos no procede por razones de interés social, de seguridad nacional, de salud pública o por afectarse derechos de terceros, en los términos que lo disponga la Ley". Art. 20. Excepcionalidad para la modificación de los datos. "Los responsables de ficheros de datos pueden negar la rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales solicitada, cuando exista una resolución judicial que determine la no	NO	Art. 3, LPDP. "Bloqueo: Es la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en el	NO

								llevará a cabo de manera gratuita para el titular".	modificación.		fichero de datos en el que se encuentran".	
Panamá	Art. 42 y 44 de la Constitución del *habeas data* distingue el derecho de toda persona a suprimir datos personales en toda base de datos o registros públicos o privados de conformidad con lo previsto en la ley. El numeral 3 del artículo 15 de la Ley 81 determina el derecho de cancelación, con un contenido similar al de rectificación, pues permite al titular solicitar la "eliminación de sus datos personales incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes". El artículo 4 de la Ley 81, señala que suprimir o borrar de forma permanente los datos almacenados en base de datos, cualquiera que sea el procedimiento empleado para ello."	El numeral 3 del artículo 15 de la Ley 81 determina el derecho de cancelación, con un contenido similar al de rectificación, pues permite al titular solicitar la "eliminación de sus datos personales incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes". Artículo 17. Los datos deberán ser modificados cuando sean erróneos, inexactos, equívocos o incompletos dentro de un término de cinco días hábiles siguientes a la solicitud, de modificación, quien sea responsable de una base de datos regulada por esta Ley, podrá proceder a la eliminación, modificación o bloqueo de los datos personales sin necesidad de requerimientos del titular, cuando existan pruebas de	SI. De acuerdo al numeral 3 del artículo 15 de la Ley 81.	SI. De acuerdo al numeral 3 del artículo 15 de la Ley 81.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	SI. Como aplicación del consentimiento, y de los principios de licitud y de veracidad y exactitud. Artículo 17. Los datos deberán ser modificados cuando sean erróneos, inexactos, equívocos o incompletos dentro de un término de cinco días hábiles siguientes a la solicitud, de modificación, quien sea responsable de una base de datos regulada por esta Ley, podrá proceder a la eliminación, modificación o bloqueo de los datos personales sin necesidad de requerimientos del titular, cuando existan pruebas de inexactitud no pueda ser establecida o cuya vigencia y respecto de los cuales no corresponda la cancelación. En este caso, serán bloqueados para acceso a terceros o para evitar su uso en otros fines que no hayan sido los expresamente autorizados.	NO.

		inexactitud no pueda ser establecida o cuya vigencia y respecto de los cuales no corresponda la cancelación. En este caso, serán bloqueados para acceso a terceros o para evitar su uso en otros fines que no hayan sido los expresamente autorizados.										
Perú	El artículo 20, LPDP, señala el derecho de supresión. Utiliza otro término similar por el cual el titular de los datos personales tiene derecho a la supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento.	Art. 20, LPDP. "[…] tiene derecho a la supresión de sus datos personales materia de tratamiento, […] cuando se hubiere advertido omisión, error o falsedad".	Según el artículo 20, LPDP, "el titular de los datos personales tiene derecho a la supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos".	NO.	NO.	Según el artículo 20, LPDP, "el titular de los datos personales tiene derecho a la supresión de sus datos personales materia de tratamiento, […] cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados".	NO.	Según el artículo 20, LPDP, "el titular de los datos personales tiene derecho a la supresión de sus datos personales materia de tratamiento, […] cuando hubiera vencido el plazo establecido para su tratamiento".	NO.	NO.	NO.	NO.	NO.
República Dominica	El artículo 5 de la Ley 172-13 recoge el principio de calidad de	NO.	El artículo 5 de la Ley 172-13	NO.	NO.	NO.	NO.	NO.	NO.	Por su parte, el artículo 15 de la Ley 172-13 señala que la	Es decir, la supresión,	NO.	NO.

na	los datos, por el cual los datos, total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso, completados por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular de los datos establecidos en la presente ley".		recoge el principio de calidad de los datos, por el cual los datos, total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso, completados por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular de los datos establecidos en la presente ley.					cancelación da lugar al bloqueo de los datos, conservándose únicamente a disposición de los poderes del Estado para la atención de las posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de estas. Cumplido el citado plazo, deberá procederse a la supresión. En todo caso, la supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.	además de un derecho del titular es un deber del responsable de la base de datos.	
Uruguay	Derecho de cancelación y bloqueo. El artículo 4° del Decreto 414/009, cuando señala las definiciones determina los conceptos de: "[...] b) cancelación o supresión de datos, que es aquel procedimiento mediante el cual el responsable cesa en el uso de los datos. La supresión o cancelación implica el bloqueo por un plazo; vencido éste se deberá proceder a su eliminación definitiva".	NO.	NO.	NO.	NO.	NO.	NO.	NO.	Según el artículo 15 de la Ley 18.331 "La rectificación, actualización, inclusión, eliminación o supresión de datos personales cuando corresponda, se efectuará sin cargo alguno para el titular".	Artículo 26. Excepciones a los derechos de acceso, rectificación y cancelación. "Los responsables dc las bases de datos que contengan los datos a que se refieren los incisos segundo y tercero del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando. Los responsables de las bases de datos de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que	NO.	El artículo 4° del Decreto 414/009, cuando señala las definiciones, determina los conceptos de: a) bloqueo de datos que es el procedimiento mediante el cual se reservan datos con el fin de impedir su tratamiento, excepto para ser puestos a disposición de los Poderes del Estado, o instituciones que estén legalmente habilitadas, a los efectos de atender las posibles responsabilidades surgidas del	Según el literal c) del artículo 4° del Decreto 414/009, cesión de datos, por la cual se comunica los datos a un tercero, dicha comunicación debe ser detenida cuando los datos se eliminan de la base original, y además debe reportarse al tercero para que también los elimine de la suya.

se refiere el inciso anterior cuando el mismo obstaculice las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el titular del dato esté siendo objeto de actuaciones inspectivas".

tratamiento.

Excepto Guatemala, los países analizados reconocen el derecho de cancelación por el cual se puede eliminar o suprimir datos personales, siempre y cuando se cumplan con las siguientes condiciones:

- *Error o falsedad:* Argentina, Ecuador, Panamá y Perú señalan que solo pueden eliminarse datos personales errados o falsos.
- *Incompletos o inexactos:* Panamá, Perú y República Dominicana requieren para que sea posible el derecho de cancelación o supresión que los datos sean inexactos o incompletos.
- *Innecesarios, impertinentes irrelevantes, desfasados, excesivos, tratados en violación a la ley o sin consentimiento*: Panamá determina la eliminación de datos personales irrelevantes, desfasados, o impertinentes. Mientras que Brasil menciona datos personales innecesarios, excesivos o tratados en violación a la ley o sin consentimiento.
- *Afecten derechos:* Colombia, Ecuador y Nicaragua determinan que pueden eliminarse datos personales cuando afecten los derechos del titular.
- *No cumplen con la finalidad:* Perú y Costa Rica consideran como condición para eliminar datos personales cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados.
- Final del procesamiento: Brasil en lugar de mencionar el cumplimiento de la finalidad lo hace respecto del procesamiento como acción real que concluida significa la terminación de un proceso.
- *Vencido el plazo para su tratamiento:* Únicamente Perú señala que pueden ser eliminados datos personales cuando se hubiera vencido el plazo establecido para su tratamiento.

Finalmente, respecto del derecho de eliminación, supresión o cancelación, varias legislaciones establecen variantes para su adecuada ejecución que se analizarán a continuación:

- *Deber del responsable del tratamiento:* República Dominicana y Costa Rica establecen que, además de un derecho del titular, es una obligación del responsable del tratamiento.
- *Gratuito:* Argentina, Brasil, Colombia, Costa Rica, Ecuador, México, Nicaragua, Panamá y Uruguay determinan que no tendrá costo para el titular la rectificación del dato personal.
- *Negativa motivada a rectificación:* Argentina, Brasil, México, Nicaragua y Uruguay establecen excepciones por las cuales el derecho de cancelación puede no cumplirse, en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando. Ecuador y Colombia, por su parte, señalan que procede la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos; en el primer caso o en el segundo cuando existe un deber legal o contractual que lo disponga. República Dominicana, entretanto, señala que la cancelación no es posible cuando existen posibles responsabilidades del tratamiento durante el plazo de prescripción de estas obligaciones. Cumplido el plazo, deberá procederse a la supresión. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos. Argentina señala también como excepciones, cuando se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de crímenes y delitos por la autoridad competente y la verificación de infracciones administrativas. Nicaragua y Argentina autorizan la negativa cuando exista una resolución judicial que lo determine. Argentina, por su parte, establece también excepciones formales, esto es si el solicitante no es titular de los datos personales, o el representante legal no esté debidamente acreditado, no se encuentren los datos personales del solicitante en la base de datos, cuando haya sido previamente realizada. Asimismo, Uruguay señala que los responsables de las bases de datos de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el inciso anterior cuando el mismo obstaculice las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias. Uruguay, Guatemala y Argentina, además, establecen que ante la negativa los titulares tienen derecho a solicitar una revisión de la negativa ante autoridad competente.
- *Bloqueo:* Argentina, Colombia, Costa Rica, México, Nicaragua y Uruguay establecen que antes de tomar la decisión de eliminar un dato y durante el tiempo de deliberación de esta decisión, el dato personal debe bloquearse y dejar constancia de ello para informar por qué no puede ser usado. Panamá en el artículo 4 de la Ley 81, menciona el bloqueo de datos, pero no como parte del derecho de cancelación sino en aplicación del consentimiento, y de los principios de licitud y de veracidad y exactitud. Brasil por su parte señala que en el compartimento de datos la eliminación o bloqueo de los datos deben ser comunicados con la finalidad de que se repita el mismo procedimiento.

- *Cesión:* Argentina y Uruguay establecen que la comunicación de datos a un tercero debe ser detenida cuando los datos se eliminan de la base original, y además debe reportarse al tercero para que también los elimine de la suya. Brasil determina que si se ha compartido datos la eliminación debe repetirse, a menos que sea imposible o conlleve un esfuerzo desproporcionado.
-

1.5.5.5 Derecho de oposición

Desde la perspectiva de la intimidad, se colige lo siguiente:

Tabla 37

País	Derecho de oposición
El Salvador	NO.
Bolivia	NO.
Chile	El consentimiento puede ser revocado sin efecto retroactivo (art. 4).
Honduras	NO.
Paraguay	NO.
Venezuela	NO.

Fuente y elaboración: La autora (2018).

De la tabla 37, se colige que aquellos países que basan el sistema de protección de los datos personales desde el derecho a la intimidad o a la privacidad no reconocen el derecho de oposición, que es contenido propio del derecho a la autodeterminación informativa. En este sentido, El Salvador, Bolivia, Honduras, Paraguay y Venezuela no incluyen este derecho. Ahora bien, Chile reconoce que el consentimiento puede ser revocado; esta es una forma indirecta de aplicación de este derecho; sin embargo, no está reconocido como tal.

a) Respecto del derecho a la protección de datos personales

Tabla 38

País	Derecho de oposición	Sin consentimiento	Motivo suficiente	Revocatoria Consentimiento	Parte deber de información	Negativa a la oposición	Cese tratamiento o supresión
Argentina	NO.	NO.	NO.	NO.	Art. 6, LPDP. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: [...] c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente (datos sensibles, art. 7). "d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos".	NO.	NO.
Brasil	NO	NO	NO	SI, Art. 18 numeral IX LGPD. El titular de los datos personales tiene derecho a obtener del controlador, en relación con los datos del titular procesados por él, en cualquier momento y previa solicitud: (…) IX - revocación del consentimiento, de conformidad con el § 5 del art. 8 de esta Ley. Artículo § 5 LPDP. "(…) El consentimiento puede ser revocado en cualquier momento por la manifestación expresa del titular, para el procedimiento de libre y fácil, ratificado los tratamientos bajo la protección del consentimiento expresado previamente, mientras que no hay ningún requisito para su eliminación de acuerdo con la sección VI de la cápita de arte. 18 de esta Ley.	SI. Art. 8 Párrafo 6 LGPD: "(…) En caso de alteración de la información referida en los ítems I, II, III o V del art. 9 de esta Ley, el controlador informará al titular, con énfasis específico en el contenido de los cambios, y el titular puede, en los casos en que se requiera su consentimiento, revocarlo si no está de acuerdo con el cambio.	NO.	SI, Art. 15 III LGPD. La conclusión del procesamiento de datos personales se producirá en las siguientes hipótesis: III - comunicación del titular, incluido el ejercicio de su derecho a revocar el consentimiento según lo dispuesto en el párrafo 5 del art. 8 de esta Ley, salvaguardando el interés público; o
Colombia	Declarado inexequible e incorporado como derecho. La Corte Constitucional sobre este literal lo declara inexequible, de tal	NO.	NO.	SI. Art. 9°, Ley 1581-2012. Revocatoria de la autorización y/o supresión del dato. "Los Titulares podrán en todo momento solicitar al	NO.	Art. 9°, Ley 1581-2012 La solicitud de supresión de la información y la revocatoria de la	Art. 9°. Ley 1581-2012. El responsable y el encargado deben poner a disposición del titular mecanismos gratuitos y de fácil acceso para presentar

	forma que el literal e) debe entenderse en el sentido de que el titular también podrá revocar la autorización y solicitar la supresión del dato, cuando no exista un deber legal o contractual que le imponga el deber de permanecer en la referida base de datos.			responsable o encargado la supresión de sus datos personales y/o revocar la autorización otorgada para el Tratamiento de los mismos, mediante la presentación de un reclamo, de acuerdo con lo establecido en el artículo 15 de la Ley 1581 de 2012".		autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos.	la solicitud de supresión de datos o la revocatoria de la autorización otorgada. Si vencido el término legal respectivo, el responsable y/o el encargado, según fuera el caso, no hubieran eliminado los datos personales, el titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales. Para estos efectos, se aplicará el procedimiento descrito en el artículo 22 de la Ley 1581 de 2012.
Costa Rica	NO.	NO.	NO.	Art. 5, Principio de consentimiento informado 2. Otorgamiento del consentimiento.- Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo.	NO.	NO.	NO.
Ecuador	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Guatemala	NO.	NO.	NO.	NO.	NO.	NO.	NO.
México	Art. 27, LFPDPPP. El titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular.	NO.	Art. 47, LPDPSO. El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando: I. Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular,	NO.	NO.	NO.	NO.
Nicaragua	Art. 34, Decreto 36-2012. Derecho de oposición. Para efectos de lo establecido en el artículo 9, párrafo segundo de la ley, el titular de los datos tiene derecho a que no se lleve a cabo el tratamiento de sus datos personales o se cese en el mismo, cuando no hubiere prestado su consentimiento para su recopilación por haber sido tomados	Art. 34, Decreto 36-2012. Derecho de oposición. Para efectos de lo establecido en el artículo 9, párrafo segundo de la ley, el titular de los datos tiene derecho a que no se lleve a cabo el tratamiento de sus datos personales o se cese en el mismo, cuando no hubiere prestado su consentimiento para su recopilación por haber sido	Art. 34, Decreto 36-2012 8 [...] Aun cuando hubiere prestado su consentimiento, el titular de los datos tiene derecho a oponerse al tratamiento de sus datos, si acredita la existencia de motivos fundados y legítimos relativos a una concreta situación personal que justifiquen el ejercicio de este derecho.	NO.	NO.	Art. 34, Decreto 36-2012 8. No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea requerido por ley.	Artículo 34, Decreto 36-2012 8. En el caso de que la oposición resulte justificada el responsable del fichero de datos deberá proceder al cese del tratamiento que ha dado lugar a la oposición

	de fuentes de acceso público.	tomados de fuentes de acceso público.					
Panamá	El numeral 4 del artículo 15 de la Ley 81 reconoce el derecho de oposición por el cual "el titular, por motivos fundados y legítimos relacionados con una situación en particular, puede negarse a proporcionar sus datos personales o a que sean objeto de determinado tratamiento, así como a renovar su consentimiento".	El numeral 4 del artículo 15 de la Ley 81 reconoce el derecho de oposición, así como a renovar su consentimiento".	NO.	SI, Además del derecho de oposición, la revocatoria existe como derecho en la normativa panameña. Art. 6 numeral 4 Ley 81 "(…) El consentimiento podrá (…) ser revocado, sin efecto retroactivo. Art. 21 LGPD "(…) El derecho del titular de los datos personales al acceso, revocación, cancelación, oposición o bloqueo de sus datos no puede ser limitado mediante ningún acto o convenio entre partes, cuyo caso se declarará nulo le acto de limitación.	NO.	NO.	NO.
Perú	Art. 22 LPDP, Siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.	Art. 22, LPDP. Siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.	Art. 22, LPDP. Siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.	NO.	NO.	Art. 22, LPDP. "[...] siempre que, por ley, no se disponga lo contrario".	Art. 22, LPDP. En caso de oposición justificada, el titular el encargado del banco de datos personales, según corresponda, debe proceder a su supresión, conforme a la ley.
República Dominicana	Art. 8, Ley 172-13. Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos, los datos personales de los que sea titular y que estén incluidos en un banco de datos.	NO.	NO.	NO.	NO.	Art. 8, Ley 172-13. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación contractual o legal de conservar los datos.	Art. 8, Ley 172-13. Durante el proceso de verificación y rectificación del error o inexactitud de la información de que se trate, el responsable o usuario del banco de datos deberá consignar, al proveer información relativa al demandante, la circunstancia de que se encuentra sometida a revisión o impugnación.
Uruguay	NO.	NO.	NO.	NO.	NO.	NO.	NO.

Fuente y elaboración: La autora (2018).

Derecho de oposición: Este derecho es el menos homogéneo de los analizados, ya que únicamente Colombia (por sentencia), México, Nicaragua, Panamá y República Dominicana lo reconocen como derecho; es decir, solo las legislaciones más modernas de Latinoamérica.
Brasil reconoce la revocatoria del consentimiento como derecho pero no la oposición como tal.

Ahora bien, esas normativas determinan las condiciones por las cuales opera el derecho de oposición y consisten en:

- *Sin consentimiento:* Nicaragua y Perú determinan que el titular de los datos tiene derecho a que no se lleve a cabo el tratamiento de sus datos personales o se cese en el mismo, cuando no hubiere prestado su consentimiento para su recopilación o por haber sido tomados de fuentes de acceso público (Nicaragua). Panamá faculta al titular a la negativa de entregar sus datos, es decir la negativa del consentimiento o de su renovación, el derecho de oposición se correlaciona directamente con el principio de consentimiento.
- *Motivo suficiente:* Nicaragua y Perú señalan que el titular de los datos tiene derecho a oponerse al tratamiento de sus datos, si acredita la existencia de motivos fundados y legítimos relativos a una concreta situación personal que justifiquen el ejercicio de este derecho. México señala que el titular podrá oponerse al tratamiento cuando es necesario evitar un daño o perjuicio al titular.

Finalmente, la normativa regula la forma de proceder del derecho de oposición y menciona lo siguiente:

- *Negativa a la oposición:* Colombia, Nicaragua, Perú y República Dominicana siempre que por ley no se disponga lo contrario. Asimismo, Colombia y República Dominicana señalan que no procederán cuando el titular tenga un deber contractual de permanecer en la base de datos. Finalmente, República Dominicana determina que la supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros.
- *Cese tratamiento o Supresión:* Colombia determina que el responsable y el encargado deben poner a disposición del titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada. Si vencido el término legal no se hubiera eliminado, el titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que la ordene.

  Nicaragua y Perú determinan que si la oposición resulta justificada, el responsable del fichero de datos deberá proceder al cese del tratamiento que ha dado lugar a la oposición.

  Por su parte, República Dominicana requiere que durante el proceso de verificación y rectificación, el responsable o usuario del banco de datos deberá proveer información sobre la circunstancia de que se encuentra sometida a revisión o impugnación.

Otras normativas lo reconocen de manera indirecta como:

- *Deber de información:* Argentina infiere del contenido de este derecho, de la mano de una interpretación del principio de información cuando se señala al recabarse datos personales, que se deberá informar previamente a sus titulares en forma expresa y clara sobre el carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga y las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos. Toda vez que el titular puede decidir oponerse a entregar sus datos personales en determinadas circunstancias.
- *Brasil como parte del derecho de información incluye la comunicación de la posibilidad del titular de revocar en cualquier tiempo y si las condiciones de recogida han cambiado.*
- *Revocatoria del consentimiento:* Colombia y Costa Rica no mencionan de forma expresa el derecho de oposición, sino el derecho de revocación, por el cual en cualquier tiempo se podrá revocar el consentimiento, de la misma forma en el que este fue obtenido; es decir, por parte del titular del dato o su representante y mediante manifestación expresa y por escrito, ya sea en un documento físico o electrónico. Brasil menciona expresa y únicamente el derecho de revocatoria en cualquier tiempo y sin necesidad de cumplimiento de ninguna condición o requisito. Mientras que Panamá reconoce el derecho de oposición y al mismo tiempo el de revocatoria, en cualquier tiempo y sin efecto retroactivo.

1.5.5.6 Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

Derecho de consulta al registro general de protección de datos personales. Desde esta perspectiva, se colige lo siguiente:

Tabla 39

País	Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales
El Salvador	NO.
Bolivia	NO.
Chile	El artículo 5 de la Ley 19628 determina que el responsable del banco de datos personales podrá "establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes".
Honduras	NO.
Paraguay	NO.
Venezuela	NO.

Fuente y elaboración: La autora (2018).

De lo analizado en la tabla 39, se infiere que únicamente Chile menciona la posibilidad de que se realicen procedimientos automatizados siempre que se protejan derechos de los titulares; esta aproximación no reconoce el derecho sino el reconocimiento de que estas formas de tratamiento pueden causar transgresiones a derechos.

a) Respecto del derecho a la protección de datos personales

Tabla 40

País	Derecho a no soportar valoraciones producto de procesos automatizados	Perfil o personalidad	Afecta derechos	Excepciones	Valor jurídico	Derecho a conocer	Impugnación
Argentina	Art. 20, núm. 1, LPDP. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado. 2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.	Suministren una definición del perfil o personalidad del interesado.	NO.	NO.	Art. 20, núm. 1, LPDP 2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.	NO.	NO.
Brasil	SI. Art. 20. LGPD "El interesado tiene derecho a solicitar la revisión de las decisiones tomadas únicamente sobre la base del procesamiento automatizado de datos personales que afecten sus intereses, incluidas las decisiones para definir su perfil personal, profesional, de consumo y de crédito, o Los aspectos de tu personalidad. (Redacción dada por la Ley N ° 13.853 de 2019) Párrafo 1. El controlador deberá proporcionar, cuando se solicite, información clara y adecuada sobre los criterios y procedimientos utilizados para la decisión automatizada, de conformidad con los secretos comerciales e industriales. Párrafo 2. En caso de que no se proporcione la información mencionada en el párrafo 1 de este artículo basada en la observancia del secreto comercial e industrial, la autoridad nacional puede realizar auditorías para verificar aspectos discriminatorios en el procesamiento automatizado de datos personales".	Art. 20 LGPD "(…) las decisiones para definir su perfil personal, profesional, de consumo y de crédito, o Los aspectos de tu personalidad.	Art. 20 LGPD "(…) que afecten sus intereses"	NO	NO	SI. Art. 20 LGPD "(…) Párrafo 1. El controlador deberá proporcionar, cuando se solicite, información clara y adecuada sobre los criterios y procedimientos utilizados para la decisión automatizada, de conformidad con los secretos comerciales e industriales.	SI. Art. 20 LGPD "(…) Párrafo 2. En caso de que no se proporcione la información mencionada en el párrafo 1 de este artículo basada en la observancia del secreto comercial e industrial, la autoridad nacional puede realizar auditorías para verificar aspectos discriminatorios en el procesamiento automatizado de datos personales".
Colombia	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Costa Rica	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Ecuador	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Guatemala	NO.	NO.	NO.	NO.	NO.	NO.	NO.

México	Art. 47, LGPDPPSO de 2017. El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando: [...] b) Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.	Art. 47, LGPDPPSO de 2017. Determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.	Art. 47, LGPDPPSO de 2017. El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando: [...] b) Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.	NO.	NO.	NO.	NO.
Nicaragua	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Panamá	Art. 19, Ley 81. El titular de los datos personales tiene derecho a no ser sujeto de una decisión basada únicamente en el tratamiento automatizado de sus datos personales, que produzca efectos jurídicos negativos o le produzca un detrimento a un derecho, cuyo objeto sea evaluar determinados aspectos de su personalidad, estado de salud, rendimiento laboral, crédito, fiabilidad, conducta, características o personalidad, entre otros. No obstante, dicha decisión será posible cuando: 1. El titular de los datos personales la haya consentido. 2. Sea necesaria para celebrar o dar cumplimiento a un contrato o relación jurídica entre el responsable del tratamiento y el titular de los datos personales. 3. Sea autorizada por leyes especiales o las normativas que las desarrollen.	Art. 19, Ley 81. "(…) Cuyo objeto sea evaluar determinados aspectos de su personalidad, estado de salud, rendimiento laboral, crédito, fiabilidad, conducta, características o personalidad, entre otros.".	SI. Art. 19, Ley 81. "(…) que produzca efectos jurídicos negativos o le produzca un detrimento a un derecho,	SI, Art. 19, Ley 81. "(…) No obstante, dicha decisión será posible cuando: 1. El titular de los datos personales la haya consentido. 2. Sea necesaria para celebrar o dar cumplimiento a un contrato o relación jurídica entre el responsable del tratamiento y el titular de los datos personales. 3. Sea autorizada por leyes especiales o las normativas que las desarrollen.	NO.	NO.	NO.
Perú	Art. 23, LPDP. Derecho al tratamiento objetivo. El titular de datos personales tiene derecho a no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, sustentada únicamente en un tratamiento de datos personales destinado a evaluar determinados aspectos de su personalidad o conducta, salvo que ello ocurra en el marco de la negociación, celebración o ejecución de un contrato o en los casos de evaluación con fines	Evaluar determinados aspectos de su personalidad o conducta.	Le afecten de manera significativa.	Art. 23, LPDP. Salvo que ello ocurra en el marco de la negociación, celebración o ejecución de un contrato o en los casos de evaluación con fines de incorporación a una	NO.	NO.	NO.

	de incorporación a una entidad pública, de acuerdo con la ley, sin perjuicio de la posibilidad de defender su punto de vista, para salvaguardar su legítimo interés.			entidad pública, de acuerdo con la ley, sin perjuicio de la posibilidad de defender su punto de vista, para salvaguardar su legítimo interés.			
República Dominicana	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Uruguay	Art. 16, Ley 18.331. Derecho a la impugnación de valoraciones personales.- Las personas tienen derecho a no verse sometidas a una decisión con efectos jurídicos que les afecte de manera significativa, que se base en un tratamiento automatizado o no de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros.	Art. 16, Ley 18.331. A evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros.	Les afecten de manera significativa	NO.	Art. 16, Ley 18.331. La valoración sobre el comportamiento de las personas, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.	Art. 16, Ley 18.331. En este caso, el afectado tendrá derecho a obtener información del responsable de la base de datos, tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto.	Art. 16, Ley 18.331. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad.

Fuente y elaboración: La autora (2018).

De lo analizado en la tabla 40, este derecho es reconocido de manera heterogénea en Argentina, Brasil, Panamá, Perú, México y Uruguay. El resto de países analizados no realizan aún aproximaciones básicas a su contenido.

Los elementos comunes del contenido de este derecho son:

- *Derecho a no soportar valoraciones producto de procesos automatizados:* Consiste en el derecho que tiene el titular derecho de no verse sometidas a una decisión con efectos jurídicos que provenga de valoraciones automatizadas. En el caso de Argentina se hace hincapié a que la valoración sea únicamente producto de proceso automatizado. Solo Argentina determina que las decisiones deben ser judiciales o relativas a actos administrativos; en el resto de legislaciones el ámbito de cobertura es amplio.
- Brasil determina un contenido distinto porque establece que el derecho consiste en solicitar la revisión de las decisiones tomadas únicamente sobre la base del procesamiento automatizado de datos personales.
  Perfil o personalidad: El proceso de automatización se refiere a la definición, extracción, análisis, evaluación (Argentina, Panamá, Perú, Uruguay) o predicción (México) del perfil, conducta o personalidad del interesado o aspectos personales (Argentina, Panamá Perú, México y Uruguay). En particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento o conducta, rendimiento laboral, crédito, entre otros (México, Panamá, Brasil y Uruguay)
- *Afecta derechos:* Uruguay y Perú señalan que el proceso de automatización afecta significativamente al titular. México, por su parte, establece efectos jurídicos no deseados o que afecte de manera significativa sus intereses, derechos o libertades. De esta forma, se establece una limitación a las valoraciones producto de procesos automatizados debido a la posibilidad de que pudieran afectar derechos fundamentales como en el caso panameño. Brasil señala una postura diferente porque habilita este derecho cuándos se afectan intereses del titular no necesariamente derechos. Finalmente, Panamá habilita otra condición relativa a que la valoración haya producido efectos jurídicos negativos para el titular.
- *Excepciones:* La de Perú determina excepciones respecto de lo negativo de realizar procesos automatizados o eliminar los resultados de esta automatización cuando ocurran en el marco de la negociación, celebración o ejecución de un contrato o en los casos de evaluación con fines de incorporación a una entidad pública, de acuerdo con la ley, sin perjuicio de la posibilidad de defender su punto de vista, para salvaguardar su legítimo interés. En el mismo sentido, Panamá, determina que la decisión automatizada es posible por disposición legal, consentimiento del titular o cuando sea necesario para celebrar o dar cumplimiento a un contrato o relación jurídica.
- *Valor jurídico:* Argentina determina que los actos que resulten contrarios a la disposición precedente serán insanablemente nulos, como forma de salvaguardar los derechos del titular. Uruguay establece, en cambio, otra forma de protección positiva, por la cual determina que la valoración sobre el comportamiento de las personas podrá tener valor probatorio únicamente a petición del afectado.
- *Derecho a conocer:* Uruguay determina que el afectado tendrá derecho a obtener información del responsable de la base de datos, tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento automatizado.

Brasil establece la obligación del responsable de tratamiento de entregar y del titular de solicitar información clara y adecuada sobre los criterios y procedimientos utilizados para la decisión automatizada.

- *Impugnación:* Finalmente, Uruguay determina que el afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración automatizada de su comportamiento. Brasil por su parte determina que la autoridad de control puede realizar auditorías para evaluar aspectos discriminatorios en el procesamiento automatizado de datos personales cuando no se cumpla con la entrega de la información.

De los pocos países que reconocen este derecho, Uruguay es el que más desarrolla los mecanismos fácticos que permiten la vigencia de este derecho, especialmente por el criterio de reversión de la carga probatoria.

1.5.5.7 Derecho a indemnización por daños causados

Desde esta perspectiva, se colige lo siguiente:

Tabla 41

País	Responsabilidad
El Salvador	El artículo 81 de la Ley 534-2011 determina la aplicación de sanciones sin perjuicio de las responsabilidades penales, civiles, administrativas o de otra índole en que incurra el responsable.
Bolivia	NO.
Chile	El artículo 23 de la Ley 19628 señala que la persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal. El artículo 11 de la Ley 19628 establece que el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.
Honduras	NO.
Paraguay	NO.
Venezuela	NO.

Fuente y elaboración: La autora (2018).

De lo analizado en la tabla 41, se concluye que El Salvador y Chile establecen responsabilidades civiles, administrativas y penales de quienes traten datos personales por los posibles daños causados que pueden generar indemnizaciones.

a) Respecto del derecho a la protección de datos personales

Tabla 42

País	Responsabilidad civil del responsable del tratamiento	Responsabilidad civil del funcionario o terceros	Independientes	Reparación integral
Argentina	En el capítulo VI sobre las sanciones administrativas consta el artículo 31 que menciona que sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; es posible la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000) a cien mil pesos ($ 100.000), clausura o cancelación del archivo, registro o banco de datos.	NO.	SI.	NO.
Brasil	Art. 42. LGPD El controlador o el operador que, debido al ejercicio de la actividad de procesamiento de datos personales, causa a terceros daños materiales, morales, individuales o colectivos, en violación de la legislación de protección de datos personales, está obligado a repararlos. Párrafo 1. Para garantizar una compensación efectiva al interesado: I - el operador es solidariamente responsable de los daños causados por el procesamiento cuando no cumple con las obligaciones de la ley de protección de datos o cuando no ha seguido las instrucciones legales del controlador, en cuyo caso el operador es igual al controlador, excepto en los casos de exclusión previstos en art. 43 de esta Ley; II - los controladores que están directamente involucrados en el tratamiento de los daños causados al interesado de forma conjunta y solidaria, excepto en los casos de exclusión previstos en el art. 43 de esta Ley. Párrafo 2. El juez, en los procedimientos civiles, puede revertir la carga de la prueba a favor del interesado cuando, en su opinión, la alegación es probable, hay una suficiencia a los efectos de producir evidencia o cuando la producción de evidencia por el interesado excesivamente costoso Párrafo 3. Las acciones de reparación por daños colectivos que tienen como objeto la responsabilidad bajo el título de este artículo pueden ejercerse colectivamente en los tribunales, observando la disposición de la legislación pertinente. Párrafo 4. Toda persona que repare el daño al titular tendrá derecho a recurrir contra las otras partes responsables, siempre que participen en el evento perjudicial.	SI. Párrafo 4. Toda persona que repare el daño al titular tendrá derecho a recurrir contra las otras partes responsables, siempre que participen en el evento perjudicial.	SI	NO. en su lugar menciona compensación efectiva.
Colombia	NO.	NO.	NO.	NO.
Costa Rica	NO.	NO.	NO.	NO.
Ecuador	La persona afectada podrá demandar por los perjuicios ocasionados.	La persona afectada podrá demandar por los	NO.	La persona afectada podrá demandar por los perjuicios ocasionados.

		perjuicios ocasionados.		El juez resolverá la causa mediante sentencia que ordenará la reparación integral. El concepto de reparación integral incluirá todas las obligaciones materiales e inmateriales que el juez determine para hacer efectiva dicha reparación. Constitución de la República del Ecuador, Registro Oficial 449, 20 de octubre de 2008. Art. 92. Ley Orgánica de Garantías y Control Constitucional.
Guatemala	Art. 61, Decreto 57-2008, 23/09/2008. Sistema de sanciones. Todo funcionario público, servidor público o cualquier persona que infrinja las disposiciones de la presente ley, estarán sujetos a la aplicación de sanciones administrativas o penales de conformidad con las disposiciones previstas en la presente ley y demás leyes aplicables. Art. 63, Procedimiento sancionatorio administrativo. Art. 64, Comercialización de datos personales. Art. 65, Alteración o destrucción de información en archivos. Art. 66, Retención de información. Art. 67, Revelación de información confidencial o reservada. Sin perjuicio de las indemnizaciones civiles.	NO.	Art. 62. Aplicación de faltas administrativas sin perjuicio de las civiles.	NO.
México	La LFPDPPP de 2010 señala que los titulares que consideren que han sufrido un daño o lesión en sus bienes o derechos, como consecuencia del incumplimiento a lo dispuesto en la presente ley por el responsable o el encargado, podrán ejercer los derechos que estimen pertinentes para efectos de la indemnización que proceda, en términos de las disposiciones legales correspondientes (art. 58). Las sanciones que se señalan en el procedimiento de sanciones se impondrán sin perjuicio de la responsabilidad civil o penal que resulte (art. 66).		La LGPDPPSO de 2017 determina que las responsabilidades que resulten de los procedimientos administrativos correspondientes, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos. Dichas responsabilidades se determinarán, en forma autónoma, mediante los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes; también se ejecutarán de manera independiente (art. 165).	NO.
Nicaragua	La Sala de lo Constitucional de la Corte Suprema de Justicia dictará sentencia en la que otorgará al recurrente el derecho a demandar el pago de daños y perjuicios ocasionados, los cuales se liquidarán mediante un proceso de ejecución de sentencia.	NO.	La Sentencia de la Sala de lo Constitucional no impide la utilización de la jurisdicción ordinaria civil y penal para ejercer los derechos mediante las acciones correspondientes. El artículo 84 duodecies de la Ley de Amparo reformada en 2013 señala que la sentencia de la Sala de lo	NO.

			Constitucional no impide la utilización de la jurisdicción ordinaria civil y penal para ejercer los derechos a través de las acciones correspondientes.	
Panamá	Art. 14, Ley 81. "(…) El custodio de la base de datos regulado por esta Ley, por encargo o mandato del responsable del tratamiento de los datos personales, así como todo aquel que tenga acceso a los datos personales por razón de su relación a nivel jerárquico, deberá cuidar de estos con la debida diligencia, ya que será igualmente responsable por aquellos daños o perjuicios ocasionados que le sean exigibles. El artículo 37, Ley 81. El responsable del tratamiento de los datos personales deberá indemnizar el daño patrimonial y/o moral que causará por el tratamiento indebido de estos, de conformidad con lo establecido en esta Ley o en el ordenamiento legal vigente. Los tribunales de justicia conocerán de las demandas que se presenten contra los responsables del tratamiento de los datos personales, así como sobre las reclamaciones por daños y perjuicios causados.	Art. 21 de la Ley 6 de 2002 determina la resolución favorable de una acción de *habeas data*, tendrá derecho a demandar civilmente al servidor público responsable por los daños y perjuicios que se le hayan ocasionado.	SI.	NO.
Perú	Derecho a indemnización por daños causados. En el artículo 25 de la Ley de Protección de Datos Personales consta el derecho a ser indemnizado, por el cual el titular de los datos personales afectado por la consecuencia del incumplimiento de la presente ley, por el responsable o por el encargado del banco de datos personales o por terceros, tiene derecho a obtener la indemnización correspondiente, conforme a ley.	NO.	NO.	NO.
República Dominicana	El artículo 16 de la Ley 172-13 determina el derecho a indemnización por parte de los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente ley sufran daños y perjuicios, tienen el merecimiento conforme al derecho común.	NO.	NO.	NO.
Uruguay	Como se analizó previamente, la Ley 18.331 determina el principio de responsabilidad, por lo tanto el titular es responsable de las conductas que violentan la presente ley y que generan responsabilidad administrativa, y en consecuencia de aquellas que se derivan de la responsabilidad civil y penal propiciada por los mismos hechos.	NO.	NO.	NO.

Fuente y elaboración: La autora (2018).

De lo analizado en la tabla 42, excepto Colombia, y Costa Rica, todos los otros países analizados consideran que ante el incumplimiento de la normativa por parte del responsable el titular tiene derecho de demandar, por vía civil, la indemnización por los daños y perjuicios causados.

Responsabilidad civil del responsable del tratamiento: Argentina, Ecuador, Guatemala, México, Nicaragua, Perú, República Dominicana y Uruguay determinan que el responsable del tratamiento al incumplir las obligaciones consagradas en las normativas de protección de datos personales, además de las responsabilidades administrativas y penales, lo será de las civiles que hubiesen causado daños a los titulares de los datos tratados. Brasil y Panamá hacen alusión exclusiva a responsabilidad civil.

Responsabilidad civil del funcionario o terceros: Panamá es el único país que expresamente reconoce el derecho de los titulares de los datos de solicitar indemnización al funcionario público que niegue el acceso de información. En el caso del Ecuador, la norma está redactada de forma amplia por lo que se entiende que los daños pueden ser causados, tanto por el responsable del tratamiento como por el funcionario público en el ejercicio de sus funciones. Brasil, sin alusión al funcionario público, menciona que toda persona que repare el daño al titular tendrá derecho a recurrir contra las otras partes responsables, siempre que participen en el evento perjudicial.

Nicaragua, México y Guatemala reconocen expresamente que los procedimientos administrativos correspondientes son independientes de los del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

Finalmente, únicamente Ecuador hace referencia a la reparación integral por la que no solo se indemniza los daños causados únicamente desde un monto económico, sino que el juez puede arbitrar otras formas de reparación que intenten volver a la situación anterior al daño en la medida de lo posible. Brasil menciona únicamente la compensación efectiva, por la cual establece solidaridad entre responsables y encargados; la reversión de la carga de prueba a favor del interesado; y, posibilidad de ejercer acciones colectivas ante tribunales;

1.5.5.8 Derecho a la confidencialidad

Desde esta perspectiva, se colige lo siguiente:

Tabla 43

País	Confidencialidad solo datos que produzcan daño al honor, la intimidad personal	Datos personales u otros
El Salvador	En el artículo 24 de la Ley 534-2011 "se entiende por información confidencial, aquella: a. La referente al derecho a la intimidad personal y familiar, al honor y a la propia imagen, así como archivos médicos cuya divulgación constituiría una invasión a la privacidad de la persona; [...] c. Los datos personales que requieran el consentimiento de los individuos para su difusión. Los padres, madres y tutores tendrán derecho de acceso irrestricto a la información confidencial de los menores bajo su autoridad parental".	Los padres, madres y tutores tendrán derecho de acceso irrestricto a la información confidencial de los menores bajo su autoridad parental
Bolivia	NO.	El Decreto Supremo 1793, relativo a las obligaciones de las entidades certificadoras, dispone en el artículo 4, el principio de confidencialidad por el cual todas las personas involucradas y que intervengan en el tratamiento de datos personales, están obligadas a garantizar la reserva de la información, incluso hasta después de finalizado su vínculo con alguna de las actividades que comprende el tratamiento, pudiendo únicamente realizar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las tareas autorizadas.
Chile	NO.	Al tenor del artículo 7, se determina que las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.
Honduras	El *habeas data* contemplado en el artículo 182 señala que puede ser presentado para exigir confidencialidad de los datos personales almacenados en cualquier archivo o registro, privado o público, que conste en medios convencionales, electrónicos o informáticos, que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen. Esta garantía no afectará el secreto de las fuentes de información periodística. En tal sentido, el derecho de confidencialidad se encuentra tutelado siempre y cuando por intermedio de él se transgredan los derechos citados.	NO.
Paraguay	NO.	NO.
Venezuela	NO.	NO.

Fuente y elaboración: La autora (2018).

El derecho de confidencialidad solo es aplicable cuando los datos que se refieren a la intimidad y la privacidad producen daños a estos derechos y al honor, conforme lo señalan Honduras y El Salvador en la tabla 43. Otros tipos de datos que se consideran confidenciales son los de niños, niñas y adolescentes por los cuales en El Salvador se menciona la autorización de sus representantes, por cuanto el ámbito de la ley se refiere exclusivamente a datos personales de menores en poder del Estado.

De otro lado, Bolivia considera confidenciales los datos personales tratados, incluso hasta después de finalizado su vínculo con alguna de las actividades que comprende el procesamiento. Chile coincide con esta postura, pero añade que están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público.

a) Respecto del derecho a la protección de datos personales

Tabla 44

País	Confidencialidad	Subsiste confidencialidad	Excepciones
Argentina	Según el artículo 10 de la LPDP (Deber de confidencialidad), "1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. [...] 2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública".	Art. 10, núm. 1, LPDP "Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos".	Art. 40, LPDP. 1. Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística. 2. Cuando un archivo, registró o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad.
Brasil	NO. No consta en la normativa brasileña alusión al derecho a la confidencialidad sino que esta se entiende desarrollada a través del principio de seguridad de los datos personales.	NO	NO
Colombia	El literal h del artículo 4 de la Ley 1581 de Protección de Datos Personales señala entre los principios para el tratamiento de datos personales el de confidencialidad, por el cual todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.	Inclusive después de finalizada.	Art. 4, lit. h, Ley 1581. "[...] no tengan la naturaleza de públicos [...] De esta forma, se considera al dato personal como de naturaleza confidencial necesitando de autorización del titular o de la ley para su cesión y difusión conforme señala el literal c) del artículo 4 en mención que se refiere al principio de libertad".
Costa Rica	Art. 3, Ley 8968. Como la obligación de los responsables de bases de datos, personal a su cargo y personal de la Prodhab, de guardar la confidencialidad principalmente ante el acceso de información de datos personales y sensibles, aun después de terminada su relación con la base.	Aun después de terminada su relación con la base.	Encausado en este criterio, el artículo 11 advierte lo mismo bajo el nombre de secreto profesional o funcional, y declara que se podrá exceptuar de esto solo bajo decisión judicial en lo estrictamente necesario.
Ecuador	LCEFEMD, Disposición general. Intimidad: El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.	NO.	NO.
Guatemala	NO.	NO.	NO.
México	Art. 21, LFPDPPP de 2010. Es aquella por la cual señala que el responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de estos; obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	

Nicaragua	Por su parte, el artículo 8 de la Ley de Protección de Datos señala que todos los datos personales solo podrán ser revelados por consentimiento del titular de los datos, por ley expresa de interés social o por mandato judicial.	NO.	Por ley expresa de interés social o por mandato judicial.
Panamá	En el artículo 44 de la Constitución panameña relativo al *habeas data* se determina que toda persona tiene derecho a que se mantenga en confidencialidad la información o datos que tengan carácter personal contenidos en bases de datos o registros públicos y privados. La Ley 81 no concibe a la confidencialidad como derecho sino como principio, tal como se analizó en línea precedente. Entonces es derechos por su reconocimiento constitucional y principio a nivel legal.	NO.	NO
Perú	Art. 17, LPDP. "Confidencialidad de datos personales. El titular del bando de datos personales, el cargado y quienes intervengan en cualquier parte de su tratamiento y están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes".	Art. 17, LPDP. "Esta obligación subsiste aun después de finalizadas las relaciones con el titular del bando de datos personales".	Art. 17, LPDP. "El obligado puede ser relevado de la obligación de confidencialidad cuando medie consentimiento previo informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública, sin perjuicio del derecho aguardar el secreto profesional. Un contenido bastante completo del derecho a la confidencialidad de los datos personales".
República Dominicana	Conforme el artículo 5 de la Ley 172-13 consta entre los principios el deber de secreto, por el cual el responsable del archivo de datos personales y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos; obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del archivo de datos personales o, en su caso, con el responsable del mismo, [...] b) Todas las personas físicas o jurídicas, las entidades públicas o privadas, debidamente reconocidas como usuarios o suscriptores de una Sociedad de Información Crediticia (SIC), que tengan acceso a cualquier información relacionada con el historial de un titular de los datos, de conformidad con esta ley, deberán guardar la debida reserva sobre dicha información y, en consecuencia, no revelará a terceras personas, salvo que se trate de una autoridad competente. Los funcionarios públicos o empleados privados que con motivo de los cargos que desempeñen tengan acceso a la información de que trata esta ley, están obligados a guardar la debida reserva, aun cuando cesen en sus funciones. c) Fuera de los fines establecidos en esta ley, se prohíbe la divulgación, la publicación, la reproducción, la transmisión y la grabación del contenido parcial o total de un reporte de cualquier tipo proveniente de una Sociedad de Información Crediticia (SIC), referente a un titular de los datos, en cualquiera de sus manifestaciones, en cualquier medio de comunicación masivo, sea impreso, televisivo, radial o electrónico.	NO.	Art. 5, Ley 172-13. Salvo que sea relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública. Atendiendo a este principio el deber de secreto contemplará además: a) El obligado será relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la seguridad nacional o la salud pública.
Uruguay	Art. 11, Ley 18.331. Principio de reserva.- Aquellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros. Las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (art. 302, Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público.	Ley 18.331. Esta obligación subsistirá aun después de finalizada la relación con el responsable de la base de datos.	Ley 18.331. Lo previsto no será de aplicación en los casos de orden de la justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular.

Fuente y elaboración: La autora (2018).

Según lo analizado en la tabla 44, excepto Guatemala, todos los países analizados, esto es Argentina, Brasil, Ecuador, Colombia, Costa Rica, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay reconocen el derecho o el principio de confidencialidad, por el cual los datos personales no pueden ser difundidos revelados.

Asimismo, Argentina, Colombia, Costa Rica, México, Perú y Uruguay señalan que la obligación de confidencialidad subsiste aun después de finalizada su relación con el titular del archivo de datos o con la base de datos.

Finalmente, constan expresamente establecidas excepciones; es decir, casos establecidos en los que el velo del secreto puede ser levantado:

- Fuentes de información periodística (Argentina)
- Autorizados por el titular (Colombia, Nicaragua y Uruguay); consentimiento previo informado (Perú).
- Autorizadas por la presente ley o por una ley específica (Argentina, Colombia y Uruguay).
- Decisión judicial (Argentina, Costa Rica, Nicaragua, Perú, República Dominicana y Uruguay).
- Datos que tengan la naturaleza de públicos (Colombia).
- Interés social (Nicaragua).
- Defensa nacional, seguridad pública o la sanidad pública (Perú y República Dominicana).

1.5.5.9 Derecho al olvido digital

Desde esta perspectiva, se colige lo siguiente:

Tabla 45

País	Derecho al olvido digital
El Salvador	NO.
Bolivia	NO.
Chile	NO.
Honduras	NO.
Paraguay	NO.
Venezuela	NO.

Fuente y elaboración: La autora (2018).

a) Respecto del derecho a la protección de datos personales

Tabla 46

País	No reconoce derecho al olvido	Si reconoce derecho al olvido
Argentina	No se reconoce derecho al olvido digital en Argentina, ya que conforme la postura jurisprudencial descrita en el caso Rodríguez, María Belén c/ Google Inc. s/daños y perjuicios, la Corte Suprema de Justicia de la Nación, 28.10.2014, negó la petición de la interpuesta, entre otros, por motivos relacionados con la determinación de la responsabilidad subjetiva de los buscadores, la validez de las notificaciones judiciales y extrajudiciales y la libertad de expresión y censura previa.	
Brasil	NO.	
Colombia	La Corte Constitucional colombiana estableció que no existe derecho al olvido por cuanto: "La Sala coincide con la decisión adoptada en la T-040 de 2013, en el sentido de considerar que la vulneración del derecho fundamental no es imputable en este caso a Google en tanto no es responsable de producir la información. Adicionalmente, estima necesario señalar que la razón para no acceder a la desindexación consiste en la protección del principio de neutralidad de la red que, solo puede ser restringida en situaciones excepcionales".	
Costa Rica		El artículo 11 del Decreto Ejecutivo 37554, reformado por el artículo 5 del Decreto Ejecutivo de 2016, bajo la rúbrica derecho al olvido consta que no se puede exceder a diez años la conservación de datos personales que puedan afectar a su titular, a partir del fin del tratamiento de los mismos, salvo disposición normativa, que por el acuerdo de partes se haya establecido otro plazo, que exista relación continuada entre las partes o que medie interés público para conservar el dato.
Ecuador	NO.	
Guatemala	NO.	
México	Es un tema de amplia discusión debido a criterios vertidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).	
Nicaragua		El artículo 10 de la LPDP señala que el titular de los datos tiene derecho a solicitar a las redes sociales, navegadores y servidores que se supriman y cancelen los datos personales que se encuentren en sus ficheros. En los casos de ficheros de datos de instituciones públicas y privadas que ofrecen bienes y servicios y que por razones contractuales recopilan datos personales, una vez terminada la relación contractual el titular de los mismos puede solicitar que se suprima y cancele toda la información personal que se registró mientras era usuario de un servicio o comprador de un bien.
Panamá	NO. Pese a lo reciente de esta normativa no se incluyó debido a los problemas evidenciados en el caso Panamá Papers.	
Perú	NO.	No consta en la normativa de protección de datos, la Dirección General de Protección de Datos Personales. En el Expediente 045-2015-JUS/DGPDP se reconoce el derecho al olvido digital y sanciona a Google Inc.

República Dominicana	NO.
Uruguay	NO.

Fuente y elaboración: La autora (2018).

Según lo analizado en la tabla 46, las Cortes de Argentina y Colombia desconocen la existencia del derecho al olvido por la dificultad de establecer determinación de la responsabilidad subjetiva de los buscadores, la validez de las notificaciones judiciales y extrajudiciales y la libertad de expresión y censura previa. En México no hay acuerdo sobre la temática y en los otros países como Uruguay, República Dominicana y Ecuador aún no se ha discutido el tema y no existe pronunciamiento judicial que marque la pauta.

Otros países como Costa Rica, Nicaragua y Perú reconocen este derecho con diferentes contenidos:

- *Tiempo adecuado de conservación del dato*: Por el contrario, Costa Rica reconoce el derecho al olvido pero con un contenido completamente alejado del generalmente aceptado, pues se refiere a que no se puede exceder a diez años la conservación de datos personales que puedan afectar a su titular, a partir del fin del tratamiento de los mismos, salvo disposición normativa, o que por el acuerdo de partes se haya establecido otro plazo, que exista relación continuada entre las partes o que medie interés público para conservar el dato. Es decir, esta norma se refiere más bien al establecimiento de un tiempo adecuado de conservación de los datos.

- *Derecho al olvido propiamente dicho:* Mientras tanto, Nicaragua es la primera norma latinoamericana que reconoce de forma expresa el derecho al olvido digital y lo configura como un derecho del titular de solicitar a las redes sociales, navegadores y servidores a que se supriman y cancelen los datos personales. En los casos de ficheros de datos de instituciones públicas y privadas que ofrecen bienes y servicios y que por razones contractuales recopilan datos personales una vez terminada la relación contractual, el titular de los mismos puede solicitar que se suprima y cancele toda la información personal que se registró.

  La Dirección General de Protección de Datos Personales en Expediente 045-2015-JUS/DGPDP reconoce el derecho al olvido digital y sanciona a Google Inc. domiciliada en Estados Unidos, obligándole a desindexar información relacionada a un juicio penal cubierto por medios de comunicación, del que nunca se le encontró responsable. La citada Dirección consideró que Google Inc. estaba debidamente notificada y plenamente obligada a respetar las leyes peruanas, incluso si era una empresa extranjera que no se encontraba domiciliada, debido a que trataba datos personales de peruanos y era accesible desde el Perú.

1.5.5.10 Spam

Desde esta perspectiva, se colige lo siguiente:

Tabla 47

País	
El Salvador	NO.
Bolivia	Art. 57, literales d) y f), Decreto Supremo 1793. Literal d) se señala que las comunicaciones por medio de correo electrónico u otro medio de comunicación digital equivalente que tengan por finalidad la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional, deberán indicar la forma, como el destinatario puede aceptar o rechazar el envío de futuras comunicaciones del remitente, para que los usuarios puedan habilitarse o deshabilitarse en el caso de que no deseen continuar recibiendo estos mensajes o correos. Asimismo, en el literal f) se registra la necesidad de que la publicidad y acceso interactivo a los sitios web del proveedor, mediante el equipo terminal o el simple registro comercial de ingreso, no conlleva a un enlace comercial del proveedor que faculte difusión posterior, sino que esta debe ser explícita y manifiestamente aceptada por suscripción.
Chile	La Ley de Protección del Consumidor, Ley 19.496, 7 de febrero de1997, reformada por la Ley 19955, artículo único 20, D.O. 14.07.2004, señala expresamente lo siguiente: Art. 28 B.- Toda comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la materia o asunto sobre el que versa la identidad del remitente y contener una dirección válida a la que el destinatario pueda solicitar la suspensión de los envíos, que quedarán desde entonces prohibidos. Los proveedores que dirijan comunicaciones promocionales o publicitarias a los consumidores por medio de correo postal, fax, llamados o servicios de mensajería telefónicos, deberán indicar una forma expedita en que los destinatarios podrán solicitar la suspensión de las mismas. Solicitada esta, el envío de nuevas comunicaciones quedará prohibido.
Honduras	NO.
Paraguay	NO.
Venezuela	NO.

Fuente y elaboración: La autora (2018).

De los países analizados en la tabla 47, Bolivia y Chile regulan el spam o correo no deseado, ninguno de ellos lo hace como forma de protección del titular de dato personal sino como forma de regulación de la sociedad de la información (Bolivia), o derechos del consumidor (Chile). Asimismo, Bolivia regula que se habilite el mecanismo para quienes no desean seguir recibiendo correos electrónicos; finalmente, Chile prohíbe el spam.

En El Salvador, Honduras, Paraguay y Venezuela no se regula sobre este particular.

a) Respecto del derecho a la protección de datos personales

Tabla 48

País	Si reconoce *spam* o correo electrónico no deseado como parte del derecho a la protección de datos personales	No se reconoce *spam* como parte del derecho a la protección de datos personales
Argentina	En el año 2003, el Juzgado Civil y Comercial Federal 3, Secretaría 6 de la Capital Federal, dictó la primera medida cautelar contra el Spam. En dicha sentencia, se determinó que en aplicación de la Ley de Protección de Datos Personales, "el juez ordenó al demandado que, al menos mientras dure el litigio, se abstenga de seguir enviándonos mensajes de correo electrónico y que por ningún motivo transfiera o ceda a terceros ningún dato personal relacionado con nosotros, incluidas nuestras direcciones de correo electrónico".	NO.
Brasil	NO	El artículo 5 del Reglamento a la Ley Marco Civil de Internet hace alusión al spam cuando señala que para la prestación adecuada de servicios y aplicaciones por parte

		del responsable de actividades de transmisión, de conmutación o de enrutamiento, en el marco de su respectiva red, y que tienen como objetivo mantener su estabilidad, seguridad, integridad y funcionalidad, será requisito técnico indispensable para el tratamiento de cuestiones de seguridad de redes, tales como restricción al envío de mensajes masivos (spam) y control de ataques de denegación de servicio.
Colombia	NO.	NO.
Costa Rica	NO.	Art. 232, Código Penal. "Instalación o propagación de programas informáticos maliciosos.- Será sancionado con prisión de uno a seis años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos. La misma pena se impondrá en los siguientes casos: [...] e) A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos".
Ecuador	NO.	Art. 50.- Ley de Comercio Electrónico y Mensaje de Datos Información al consumidor.- En la prestación de servicios electrónicos en Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento. [...] En el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o por medio listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos. La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se sancionará de acuerdo con lo dispuesto en la presente ley. El usuario de redes electrónicas podrá optar o no por la recepción de mensajes de datos que, en forma periódica, sean enviados con la finalidad de informar sobre productos o servicios de cualquier tipo.
Guatemala	NO.	NO.
México	NO.	NO.
Nicaragua	El artículo 26 de la Ley de Protección de datos personales, sobre el envío de publicidad no deseada, señala que deberá ofrecerse la posibilidad al destinatario titular de datos personales de expresar su negativa a seguir recibiendo envíos publicitarios y promocionales de bienes y servicios o, en su caso, revocar su consentimiento de una forma clara y gratuita.	NO.
Panamá	NO	La Autoridad Nacional para la Innovación Gubernamental encabeza el CSIRT Panamá, el cual mediante aviso 2014-07– Correos no deseados (*spam*) de 15 de abril de 2014 determina criterios que deben ser aplicados por usuarios de sistema de correo electrónico para evitar *spam.*
Perú	NO.	Ley 28493, publicada en el Diario Oficial El Peruano, 12 de abril del 2005, Ley que Regula el Uso del Correo Electrónico Comercial No Solicitado (Spam).
República Dominicana	NO.	NO.
Uruguay	No consta normativa específica sobre correos no deseados. Sin embargo, la Unidad Reguladora y	NO.

	de Control de Datos Personales del Uruguay en su informe digital, esto es Spam, informe sobre correo basura, señala expresamente que: "En Aplicación de la Ley 18.331 de Protección de Datos Personales y Acción de *Habeas Data* en casos de SPAM En el ámbito de la protección de datos, la práctica de spam contraviene fundamentalmente el principio del previo consentimiento informado, debido a la obtención y utilización de información personal sin autorización de sus titulares, y las disposiciones relativas a la publicidad, al ignorar el ejercicio del derecho de retiro o bloqueo de sus datos".

Fuente y elaboración: La autora (2018).

De acuerdo con lo analizado en la tabla 48, Argentina, Nicaragua y Uruguay reconocen al *spam* o envío de correo masivo no deseado como parte del derecho a la protección de datos personales. El primero, Argentina lo ha reconocido mediante una resolución judicial. Nicaragua lo consagra en la normativa sobre protección de datos personales vigente. Uruguay lo hace por medio de la Unidad Reguladora y de Control de Datos Personales de Uruguay, la cual ha dictado un informe sobre la necesidad de consentimiento informado y la posibilidad de solicitar la eliminación de listas de correos mediante denuncias a esta unidad.

Por su parte, Guatemala, Colombia y República Dominicana no regulan el spam de ninguna manera, ni mediante normas de consumidor, ni de sociedad de información ni de telecomunicaciones.

Reconocen formas de protección al spam como parte de otros derechos o normativas: Costa Rica, Ecuador, Panamá, México y Perú.

- *Como tipo penal:* Costa Rica, en el artículo 232 de su Código Penal, prohíbe el envío masivo de comunicaciones.
- *Como mecanismo de comercio electrónico:* Ecuador, en el artículo 50 de la Ley de Comercio Electrónico y Mensaje de Datos Información al Consumidor, determina que el envío periódico de mensajes de datos no deseados debe viabilizar la exclusión de las listas.
- *Como derecho del consumidor:* En México no consta referencia sobre este tema ni en la Constitución mexicana ni en la LFTAIP, reformada en 2017, ni en LGTAIP de 2015, ni en la LFPDPPP de 2010. Esto se debe a que este tema se aborda desde la perspectiva del derecho al consumidor; incluso se ha configurado un tipo penal. Por su parte, Perú dicta la Ley 28493, 12 de abril del 2005, Ley que regula el uso del correo electrónico comercial no solicitado (*spam*), establece al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi) como la autoridad competente para velar por el cumplimiento de la citada ley.
- *Como criterio técnico de seguridad:* Panamá, la Autoridad Nacional para la Innovación Gubernamental encabeza el CSIRT Panamá, mediante aviso 2014-07- Correos no deseados (SPAM), 15 de abril de 2014; determina criterios que deben ser aplicados por usuarios de sistema de correo electrónico para evitar *spam*.
- Como criterio para prestación adecuada de transmisión: Brasil a través del Marco civil de internet establece como criterio para la prestación adecuada de las actividades de transmisión la restricción del envío masivo de mensajes.

1.5.5.11 Otros derechos

Desde esta perspectiva, se colige lo siguiente:

Tabla 49

País	Derecho de divulgación	Derecho de consulta
El Salvador	NO.	El artículo 35 de la Ley 534-2011 señala que los entes obligados que posean, por cualquier título, registros o sistemas de datos personales, o que quieran suprimirlos deberán poner en conocimiento del Instituto de Acceso y Transparencia, una lista actualizada de los mismos y de la información general sobre sus protocolos de seguridad.
Bolivia	NO.	NO.
Chile	NO.	Conforme consta en el artículo 22, se determina que será el Servicio de Registro Civil e Identificación el que llevará un registro de los bancos de datos personales a cargo de organismos públicos. Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende, todo lo cual será definido en un reglamento. El organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca. Como se ve, la obligación de registro es exclusiva de la autoridades públicas ante un organismo limitado únicamente a registrarla y que no puede realizar ningún tipo de acción de resguardo, prevención o protección con tal registro, menos aún ponerlo como parte de un derecho de consulta vinculante para el titular como para el responsable.
Honduras	Acorde con lo establecido en el artículo 22 de la Ley 8968, la Prodhab elaborará una estrategia de comunicación que permita que los administrados conozcan los derechos y mecanismos de defensa que tienen derivados del manejo de sus datos personales, mediante actividades de divulgación. Además, promoverá la protección de dicha información entre las personas o empresas que la recolecten.	NO.
Paraguay	NO.	NO.
Venezuela	NO.	NO.

Fuente y elaboración: La autora (2019).

De lo señalado en la tabla 49, se concluye que por regla general no se acepta como titular del derecho a la intimidad a las personas jurídicas, sean estas públicas o privadas, porque la forma de protección de los datos está atada al derecho a la intimidad que por su naturaleza propia es solo titular la persona natural.

b) Respecto del derecho a la protección de datos personales

Tabla 50

País	Derecho de divulgación	Derecho de revocar	Derecho de Consulta al registro general de protección de datos personales	Derecho a la tutela	Derecho a impedir suministro o a comunicar datos (Cesión)	Derecho de inclusión	Limitación del tratamiento	Derecho de portabilidad	Derecho de confirmación de existencia de tratamiento	Derecho de anonimato y bloqueo	Derecho de información sobre uso compartido de datos
Argentina	NO.	NO.	Según el artículo 21, LPDP, todo archivo, registro, base o banco de datos públicos, y privados destinados a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control. Y deberá comprender como mínimo la siguiente información: a) Nombre y domicilio del responsable; b) Características y finalidad del archivo; c) Naturaleza de los datos personales contenidos en cada archivo; d) Forma de recolección y actualización de datos; e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos; f) Modo de interrelacionar la información registrada; g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; h) Tiempo de conservación de los datos; i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos. Existe prohibición expresa respecto a que ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro. Entretanto, el artículo 31 del Decreto Nacional 1.558/2001 desarrolla infracciones, multas, responsabilidades y la obligatoriedad de realizar inspecciones. Y el artículo 24 señala que los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal están obligados también a registrar.	NO.	NO.	NO.					
Brasil	NO	SI. Art. 15. La conclusión del procesamiento de datos personales se producirá en las siguientes	SI Artículo 37 LGPD.-. El controlador y el operador deberán mantener un registro de las operaciones de procesamiento de datos personales que realizan, especialmente cuando se basan en intereses legítimos.	NO	NO	NO	SI. El artículo 6 de la LGPD señala el principio de necesidad por el cual se limita	SI. Art. 18 V LGPD.- "(...) portabilidad de los datos a otro proveedor de servicios o	SI. Art. 18 I - LGPD.- "(...) confirmación de la existencia de	SI. Art. 18 IV LGPD.- "(...) anonimato, bloqueo o eliminación de datos	SI. Art. 18 VII LGPD.- "(...) información sobre entidades públicas y privadas con las cuales el controlador

		hipótesis: III - comunicación del titular, incluido el ejercicio de su derecho a revocar el consentimiento según lo dispuesto en el párrafo 5 del art. 8 de esta Ley, salvaguardando el interés público; o						“el tratamiento al mínimo necesario para la realización de sus fines, con cobertura de los datos pertinentes, proporcionados y no excesivos en relación con los fines del tratamiento de datos”.	productos, previa solicitud expresa, de conformidad con los reglamentos de la autoridad nacional, sujeto a secretos comerciales e industriales; (...)”	tratamiento;	innecesarios, excesivos o tratados en violación de las disposiciones de esta Ley;	hizo uso compartido de datos;
Colombia	NO.	NO.	El artículo 25, LPDP, “declara que el Registro Nacional de Bases de Datos, que es el directorio público de las bases de datos sujetas a tratamiento que operan en Colombia, será administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos. Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes”.	NO.	NO.	NO.					
Costa Rica	Art. 22, Ley 8968. Derecho de divulgación. La Prodhab elaborará una estrategia de comunicación que permita que los administrados conozcan los derechos y mecanismos de defensa que tienen derivados del manejo de sus datos personales, mediante actividades de divulgación. Además, promoverá la	Art. 7 del reglamento, Decreto Ejecutivo 37554. Derecho de revocar. El titular puede revocar el consentimiento para el tratamiento de sus datos personales, en cualquier momento mediante mecanismos ofrecidos por el responsable. Cuando este haya recibido la solicitud de revocación contará	Según el artículo 44 del reglamento, Decreto Ejecutivo 37554, las personas físicas o jurídicas propietarias de bases de datos personales deberán inscribirlas mediante un registro ante la Agencia, suministrando la siguiente información: solicitud del propietario físico o jurídico, debidamente autenticado notarialmente o confrontada la firma. Añadiendo que en el caso de persona jurídica deberá presentarse personería jurídica vigente con máximo un mes de haber sido expedida; designación del responsable de la base de datos personales ante la Agencia y ante terceros, con indicación del medio y lugar de contacto, así como carta de aceptación del cargo; también identificación de los encargados, incluyendo sus datos de contacto, así como carta de aceptación del cargo; además nombres de las bases de datos y su ubicación física; especificación de las finalidades y los usos previstos; tipos de datos personales sometidos a tratamiento en	NO.	NO.	NO.					

	protección de dicha información entre las personas o empresas que la recolecten.	con cinco días hábiles para proceder conforme a esta, y deberá informales de dicho proceso a todas aquellas personas físicas o jurídicas a quienes se les haya transferido los datos para que ejecuten de igual manera la revocación del consentimiento durante cinco días hábiles, según el artículo 8 que también afirma que la revocación no tendrá efecto retroactivo.	dichas bases de datos; procedimientos de obtención de los datos personales; descripción técnica de las medidas de seguridad que se utilizan en el tratamiento de los datos personales; los destinatarios de transferencias de los datos personales; copia de los protocolos mínimos de actuación, listado de los contratos globales y ventas de ficheros vigentes, así como indicación de la estimación pecuniaria de cada uno de esos contratos; señalamiento de fax o correo electrónico para recibir notificaciones de la Agencia. Asimismo, el responsable deberá mantener el registro de la base de datos, en todo momento, actualizados ante la Agencia. Sin embargo, no serán sujetas de inscripción ante la Agencia, las bases de datos personales, internas o domésticas.				
Ecuador	NO.	NO.	NO.	NO.	NO.	NO.	
Guatemala	NO.	NO.	La información publicada en sistemas de información electrónicos deberá coincidir exactamente con los sistemas de administración financiera, contable y de auditoria del Estado por el ámbito público de la Ley en Guatemala. Por lo que, se entiende una forma de registro y consulta.	NO.	NO.	NO.	
México	NO.	NO.	NO.	NO.	NO.	NO.	
Nicaragua	NO.	NO.	El artículo 16 de la Ley 787-2012 señala el derecho a solicitar información a la Dirección de Protección de Datos Personales, relativa a la existencia de ficheros de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita, lo cual da cuenta de la obligación que tienen los responsables de ficheros de datos de inscribir en el Registro de ficheros de datos de la Dirección de Protección de Datos Personales, conforme consta en el artículo 22 de la citada ley. El artículo 23 señala que tanto los ficheros de datos públicos como los privados solo pueden crearse, modificarse o extinguirse por medio de disposiciones establecidas en dicha ley.	NO.	NO.	NO.	
Panamá	NO.	NO.	El artículo 31 de la Ley 81 determina que los responsables llevarán un registro de la bases	NO.	NO.	NO.	Art. 15 numeral 5 LGPD.

		de datos que puedan cederse a terceros, las que deberán estar a disposición de la Autoridad Nacional de Transparencia y Acceso de la Información.			"(...)Derecho de portabilidad: derecho a obtener una copia de los datos personales de manera estructurada, en un formato genérico y de uso común, que permita ser operado por distintos sistemas y/o transmitirlos a otro responsable, cuando: a. El titular haya entregado sus datos directamente al responsable. b. Sea un volumen relevante de datos, tratados de forma automatizada. c. El titular haya dado su consentimiento para el tratamiento o se requiera para ejecución o el cumplimiento de un contrato. En todo momento, el titular de los datos personales podrá ejercer estos derechos, los cuales son irrenunciables, salvo las excepciones establecidas en leyes especiales.
Perú	NO.	El artículo 34, LPDP, señala la "creación de la Autoridad Nacional de Protección de Datos Personales, cuya finalidad es recibir el Registro Nacional de Protección de Datos Personales de los bancos de datos personales de administración pública o privada, así como los datos relativos a estos que sean	Derecho a la tutela. Art. 24, LPDP. "Derecho a la tutela, por el cual el titular o el	Derecho de impedir el suministro. Art. 21. Derecho a impedir que sean suministrados sus	

			necesarios para el ejercicio de los derechos que corresponden a los titulares de datos personales, conforme a lo dispuesto en esta Ley y en su reglamento".	encargado del banco de datos personales que deniegue al titular de datos personales, total o parcialmente, el ejercicio de los derechos establecidos en esta Ley, puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de hábeas data".	datos personales, especialmente cuando ello afecte sus derechos fundamentales. El derecho a impedir el suministro no aplica para la relación entre el titular del banco de datos personales y el encargado del banco de datos personales para los efectos del tratamiento de estos. Se refiere a lo que en otras legislaciones se denomina cesión de datos personales.	
República Dominicana	NO.	NO.	NO.	NO.	NO.	NO.
Uruguay			Art. 28, Ley 18.331. Exclusivamente para la creación, modificación o supresión de bases de datos de carácter personal de titularidad privada, que no sean para un uso exclusivamente individual o doméstico, se ha previsto que las personas físicas o jurídicas privadas deberán registrarse en el Registro que al efecto habilite el Órgano de Control (art. 29). De esta forma, no consta como derecho de consulta sino como obligación de registro de los responsables de bases de datos. Para lo cual, se necesitará de la identificación de la base de datos, su responsable, la naturaleza de los datos que contiene, los procedimientos de obtención y tratamiento de datos, las medidas de seguridad, los derechos de los titulares, sus procedimientos, formas y condiciones de interposición, el destino de los datos y personas físicas o jurídicas a las que pueden ser transmitidos, el tiempo de conservación de los datos (art. 29), incluidos los cinco años previstos para bases crediticias (art. 22). De esta manera, se controlará que ningún usuario de datos posea datos personales de naturaleza distinta a los declarados en el registro. En caso de incumplimiento, podrán producirse sanciones administrativas (art. 29). El Decreto 414/009 admite como actos y		Derecho a la comunicación de datos. La Ley 18.331 establece un derecho referente a la comunicación de datos, por el cual los datos personales objeto de tratamiento solo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario, y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los	Derecho de inclusión. La Ley 18.331 no menciona el derecho de inclusión, pero el Decreto 414/009 en el artículo 12 señala que el titular tendrá derecho a incorporar una información correspondiente en una base de datos cuando acredite un interés fundado.

documentos inscribibles, aquellos que provienen de bases de datos cuyos responsables sean personas jurídicas públicas, estatales o no, y no solo los de naturaleza privada. No existiendo ámbito personal o doméstico para las personas jurídicas. Además, deberán constar en el registro los códigos de conducta de práctica profesional que establezcan normas para el tratamiento de datos personales y para las autorizaciones de transferencias internacionales de datos personales (art. 15). El plazo de inscripción será de máximo de 90 días a partir del inicio de sus actividades (art. 17°). La fecha de la inscripción se computará como fecha de inscripción definitiva, aunque la resolución de la URCPD sea posterior. Los responsables de bases de datos de carácter personal deberán exhibir en un lugar visible accesible a los usuarios el número y fecha de la citada resolución (art. 19°). La actualización del registro es obligatoria, comunicándola trimestralmente (art. 20°).

elementos que permitan hacerlo (art. 17).

De las normativas analizadas en la tabla 50, emergen derechos que no son parte habitual de las legislaciones de protección de datos personales y que se consideran innovaciones de cada país y atienden a condiciones propias de cada sociedad:

- *Derecho de divulgación:* Consagrado en Costa Rica, por el cual el organismo encargado de la protección de los datos personales en dicho país, es decir el Prodhab, elaborará una estrategia de comunicación que permita que los ciudadanos conozcan los derechos y mecanismos de defensa derivados del manejo de sus datos personales.
- *Derecho de revocar:* Reconocido en Costa Rica, mediante el cual el titular puede revocar el consentimiento para el tratamiento de sus datos personales, en cualquier momento mediante mecanismos ofrecidos por el responsable.
- *Derecho de consulta al registro general de protección de datos personales:* Este derecho podría considerarse común, ya que varios países latinoamericanos como Argentina, Brasil, Colombia, Costa Rica, Guatemala, Panamá, Perú, Nicaragua y Uruguay reconocen el derecho de consulta o registro. Este derecho determina que la creación, modificación o supresión de bases de datos personales deberán registrarse en el Registro a cargo de la entidad de protección de cada país: los responsables, la naturaleza de los datos que contiene, los procedimientos de obtención y tratamiento de datos, las medidas de seguridad, los derechos de los titulares, sus procedimientos, formas y condiciones de interposición, el destino de los datos y personas físicas o jurídicas a las que pueden ser transmitidos, el tiempo de conservación de los datos. Esto con la finalidad de que el Órgano de Control pueda controlar que ningún usuario de datos posea datos personales de naturaleza distinta a los declarados en el registro. En caso de incumplimiento podrán producirse sanciones administrativas.
- *Derecho a la tutela:* Perú determina este derecho, por el cual el titular o el encargado del banco de datos personales que deniegue al titular de datos personales, total o parcialmente, el ejercicio de los derechos establecidos en esta ley, puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de *habeas data*.
- *Derecho a impedir suministro o a comunicar datos (Cesión):* Perú y Uruguay incluyen en su normativa este derecho que impide el suministro de datos a otros; se refiere a lo que en otras legislaciones se denomina cesión de datos personales. El avance de esta legislación se refiere a conceptualizar la cesión como derecho a diferencia de la mayoría de legislaciones que la toman como forma de tratamiento, o que lo contemplan dentro de las condiciones del consentimiento.
- *Derecho de inclusión:* Uruguay consagra este derecho que consiste en que el titular tendrá derecho a incorporar una información correspondiente en una base de datos cuando acredite un interés fundado.
- *Limitación del tratamiento:* Brasil que aprobó su normativa en 2019 incluye este nuevo derecho por el cual el tratamiento debe reducirse al mínimo necesario para la realización de los fines para los cuales fue recopilado el dato. De tal manera que los datos deben ser pertinentes, proporcionados y no excesivos.
- *Derecho de portabilidad:* Brasil y Panamá son los primeros países latinoamericanos en reconocer a la portabilidad como derecho. Brasil Esto establece el derecho a la portabilidad de los datos a otro proveedor de servicios. Mientras que Panamá establece el derecho a obtener una copia de los datos personales que luego pueda ser

transmitido a otro en virtud de que tiene formato interoperable. Esta normativa establece una serie de condiciones para que la portabilidad opere.

- *Derecho de confirmación de existencia de tratamiento:* Este derecho está reconocido expresamente en la normativa brasileña y aunque pareciera que es parte del derecho de acceso o incluso del derecho de transparencia o información, los legisladores han preferido marcarlo de forma clara e independiente debido a la dificultad práctica del ciudadano de encontrar respuestas en las instituciones públicas o privadas respecto de obtener información certeza de la realización y tipo de tratamiento al que se están sometiendo sus datos personales.
- *Derecho de anonimato y bloqueo:* Si bien este derecho consta en el texto de la normativa junto al de eliminación ya que se complementan y emparejan; el legislador brasileño lo ha mencionado expresamente precisamente para visibilizar el derecho que tienen los titulares de usar internet y las tic de forma libre e independiente de injerencias estatales o de terceros.
- *Derecho de información sobre uso compartido de datos*: Este derecho reconocido en la normativa brasileña está asociado al derecho de información, por el cual las personas necesitamos conocer que datos se han compartido con otros responsables de tratamiento para de ser el caso revocar el consentimiento o ejercer otros derechos.

1.5.6 Procedimientos administrativos

Desde esta perspectiva, se colige lo siguiente:

Tabla 51

País	
El Salvador	El artículo 36 de la Ley 534-2011 dispone que los titulares de los datos personales o sus representantes, previa acreditación, podrán solicitar a los entes obligados, mediante la solicitud de información constante en el artículo 66 de la citada ley, esto es por solicitud dirigida al Oficial de Información; una solicitud en forma escrita, verbal, electrónica o por cualquier otro medio idóneo, de forma libre o en los formularios que apruebe el Instituto, lo siguiente: a. La información sobre la persona; b. Informe sobre la finalidad para la que se ha recabado tal información; c. La consulta directa de documentos, registros o archivos que contengan sus datos que obren en el registro o sistema bajo su control; d. La rectificación, actualización, confidencialidad o supresión de la información que le concierna, según sea el caso, y toda vez que el procedimiento para tales modificaciones no esté regulado por una ley especial. Recurso de apelación: Contra la negativa de entrega de informes, o de la consulta directa, rectificación, actualización, confidencialidad o supresión de datos personales, procederá la interposición del recurso de apelación ante el Instituto conforme el artículo 82. Asimismo, cuando la dependencia o entidad no entregue al solicitante los datos personales solicitados, o lo haga en un formato defectuoso o incomprensible, se niegue a efectuar modificaciones o correcciones a los datos personales, no esté conforme con el tiempo, el costo o la modalidad de entrega; la información entregada sea incompleta o no corresponda a la información requerida en la solicitud. También procederá dicho recurso en el caso de falta de respuesta en los plazos a que se refiere el artículo 36, esto es sobre informes finalidades, recursos en general, de conformidad con lo dispuesto en el artículo 38 de la Ley 534-2011. Denegatoria del recurso de apelación: Quedarán a salvo las demás acciones previstas por la ley, al tenor de lo dispuesto en el artículo 39 de la citada ley. Deberá presentarse el recurso por escrito, de forma libre o en los formularios que apruebe el Instituto. El Oficial de Información deberá remitir la petición y el expediente al Instituto a más tardar el siguiente día hábil de haberla recibido. Podrán interponerse además medidas cautelares (art. 85, Ley 534-2011).
Bolivia	NO. La Constitución Política del Estado de 1967 determinaba al *habeas data* como acción constitucional; posteriormente la vigente Constitución de 2009, en el capítulo segundo relativo a las Acciones de Defensa consagra la denominada Acción de Protección de Privacidad, constante en los artículos 130 y 131 con un contenido casi idéntico a su predecesora.
Chile	Art. 12, Ley 19628. Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente. En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen. Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento

	carezca de fundamento legal o cuando estuvieren caducos. Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal. En el caso de los incisos anteriores, la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita solo podrá ejercerse personalmente. Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos.
Honduras	NO. Conforme señala el artículo 182 de la Constitución hondureña, procede el *habeas data* para obtener acceso a la información; impedir su transmisión o divulgación; rectificar datos; actualizar información, exigir confidencialidad y su eliminación. Pero señala expresamente que los datos deben ser inexactos o erróneos o la información falsa; así como que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen.
Paraguay	NO. La norma constitucional, art. 135, fija que se podrá solicitar *habeas data*, es decir actualización, la rectificación o la destrucción de datos, si fuesen erróneos o afectaran ilegítimamente sus derechos ante el magistrado competente. Sobre este procedimiento se describirá más ampliamente en la parte relativa a procedencia y procedimiento del *habeas data*.
Venezuela	NO. A continuación se describirá el procedimiento constitucional desarrollado jurisprudencialmente a través de la sentencia de aplicación obligatoria, Resolución 1511/2009, de 9 de noviembre en el caso “Mercedes Josefina Ramírez en Acción de *Habeas Data*”.

Fuente y elaboración: La autora (2018).

Ver análisis indicado en la tabla 51 y en la tabla 52.

a) Respecto del derecho a la protección de datos personales:

Tabla 52

País	Acceso o consulta	Reclamos al responsable	Reclamos ante el órgano de control	Por vía judicial, *habeas data* legal	Procedibilidad de los reclamos al responsable	Procedibilidad de los reclamos ante el órgano de control	Procedibilidad por vía judicial, *habeas data* legal
Argentina	Art. 14, LPDP. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales a los responsables de los bancos de datos públicos, o privados. Esta petición deberá ser satisfecha dentro de los diez días después de haber sido intimado fehacientemente el responsable de la base de datos.	Art. 16, LPDP. Los derechos de rectificación, actualización o supresión podrán ser presentados ante el responsable, quien deberá realizar todas las operaciones necesarias dentro del plazo máximo de cinco días hábiles de recibido el reclamo.	NO.	Art. 16, LPDP. El incumplimiento de esta obligación dentro del término, habilita a presentar la acción de protección de los datos personales o de *habeas data* legal.	Art. 14, LPDP. Si el responsable o usuario no proporciona la información solicitada dentro de los diez días corridos de haber sido requerido o si evacuado el informe, este se estimara insuficiente, se podrá presentar acción de protección de los datos personales o de *habeas data* legal.	NO.	Art. 33.- 1. "La acción de protección de los datos personales o de hábeas data procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización".
Brasil	NO	Artículo 18. Párrafo 3 LGPD.- "(...) Los derechos previstos en este artículo se ejercerán previa solicitud expresa del titular o representante legalmente constituido, el agente de procesamiento.	Art. 55 numeral V LGPD "(...)- considerar las peticiones del titular al controlador después de que el titular evidencia la presentación de una queja al controlador que no se resuelve dentro del período establecido por la regulación; (...)"	Artículo 22. La defensa de los intereses y derechos de los interesados puede ejercerse en los tribunales, individual o colectivamente, de conformidad con las disposiciones de la legislación pertinente, en relación con los instrumentos de protección individual y colectiva.	NO	NO	NO
Colombia	Art. 14, Ley 1581. Los titulares o sus causahabientes podrán consultar la información personal del titular que repose en cualquier base de datos, sea esta del sector público o privado. El responsable o el encargado del tratamiento deberán suministrar la información por medio habilitado para el efecto en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en	Reclamos: Art. 15, Ley 1581. El titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley, podrán presentar un reclamo ante el responsable del tratamiento o el encargado del tratamiento.	NO.	NO.	Procedibilidad. El artículo 16 de la Ley 1581 señala al agotamiento de vía como requisito de procedibilidad. El titular o causahabiente, antes de acudir y presentar reclamo ante la Superintendencia de Industria y Comercio, debe elevar queja ante el responsable o el encargado del tratamiento.	NO.	NO.

	ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.					
Costa Rica	Art. 16, Decreto Ejecutivo 37554, Medios y formas para el ejercicio de los derechos. El responsable deberá poner a disposición del titular, los medios y formas simplificadas de comunicación electrónica u otros que considere pertinentes para facilitar a los titulares el ejercicio de sus derechos. Art. 21. Derecho de acceso a la información. El titular tiene derecho a obtener del responsable, la información relacionada con sus datos personales, entre ellos lo relativo a las condiciones, finalidad y generalidades de su tratamiento.	Art. 18, Decreto Ejecutivo De las solicitudes del titular hacia el responsable. El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos personales del titular. El plazo para que se atienda la solicitud será de cinco días hábiles, contados a partir del día siguiente en que la misma haya sido recibida por el responsable, en cuyo caso este anotará en el acuse de recibo que entregue al titular, la correspondiente fecha de recepción. El plazo señalado se interrumpirá en caso de que el responsable requiera información adicional al titular.	Art. 13, Ley 8968. Garantías efectivas. Toda persona interesada tiene derecho a un procedimiento administrativo sencillo y rápido ante la Prodhab, con el fin de ser protegida contra actos que violen sus derechos fundamentales reconocidos por esta ley. Lo anterior sin perjuicio de las garantías jurisdiccionales generales o específicas que la ley establezca para este mismo fin.	NO.	Art. 24, Decreto Ejecutivo. Requisitos para el ejercicio del derecho de rectificación. La solicitud de rectificación indicará a qué datos personales se refiere, así como la corrección que se solicita realizar y deberá ser acompañada de la documentación o prueba pertinente que ampare la procedencia de lo solicitado. El responsable ofrecerá mecanismos que faciliten el ejercicio de este derecho en beneficio del titular.	Art. 22, Decreto Ejecutivo. Negativa por parte del responsable. El responsable que niegue el ejercicio de cualquier gestión del titular deberá justificar por escrito su respuesta. Si el titular lo considera pertinente, podrá acudir ante la Agencia conforme el capítulo VII "De la Protección de Derechos ante la Agencia" de este reglamento.	NO.
Ecuador	NO. Solo acción constitucional de *habeas data*.						
Guatemala	NO.						
México	NO.	LFPDPPP de 2010. Ejercicio de los Derechos de Acceso, rectificación, cancelación y oposición conforme la LFPDPPP de 2010. El titular o su representante legal podrán solicitar al responsable en cualquier momento los derechos ARCO (art. 28). Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la presente Ley. Asimismo fomentará la protección de datos personales al interior de la organización (art. 30). LGPDPPSO de 2017. Los titulares previa acreditación de su identidad o representación de menores de edad o de personas fallecidas solicitarán a los sujetos obligados descritos en el artículo 1 de la citada ley, son cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y	El artículo 45 LFPDPPP de 2010 establece el procedimiento de protección de derechos, por el cual se protegerán los derechos ARCO; esto es acceso, rectificación, cancelación u oposición. Se iniciará a instancia del titular de los datos o de su representante legal cuando el responsable no entregue al titular los datos personales solicitados; lo haga en un formato incomprensible, o se niegue a efectuar modificaciones o correcciones a los datos personales.	NO.	Art. 29, LFPDPPP de 2010. El procedimiento es directo; es decir, la petición o solicitud deberá presentarse directamente a cada responsable de fichero o base de datos. Art. 56, LGPDPPSO de 2017. Recurso de revisión. Contra la negativa de dar trámite a toda solicitud para el ejercicio de los derechos ARCO o por falta de respuesta del responsable, procederá la interposición del recurso de revisión a que se refiere el artículo 94 de la presente ley. Art. 117, LGPDPPSO de 2017. Recurso de inconformidad. Podrá impugnarse la resolución del recurso de revisión emitido por el organismo garante ante el Instituto, mediante el	Art. 45, LFPDPPP. Este procedimiento es indirecto y de alzada ante la negativa o no contestación de la solicitud previa realizada directamente al responsable. Por ello, se iniciará ante el Instituto dentro de los quince días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable o en el caso de que el titular de los datos no reciba respuesta cuando haya vencido el plazo de respuesta previsto para el responsable. La solicitud de protección de datos también procederá cuando el responsable no entregue al titular los datos personales solicitados; o lo haga en un formato incomprensible, se niegue a efectuar modificaciones o correcciones a los datos personales, o el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponda a la información requerida.	NO.

		fondos públicos (art. 49). Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, el ejercicio de los derechos ARCO ante la Unidad de Transparencia del responsable, que el titular considere competente (art. 52).			recurso de inconformidad.	
Nicaragua	El artículo 18 establece que la respuesta a la solicitud de información debe ser clara y sencilla, accesible al conocimiento de la población y al titular de los datos personales; ser amplia y pertenecer al titular. Si la solicitud que tuviere fuese negativa, el artículo 13 del Reglamento a la Ley delimita que el titular de datos podrá presentar ante la DIPRODAP la denuncia correspondiente.	Los reclamos que se realizan en virtud de la Ley 787-2012 se dirigen, en primer lugar, al responsable del fichero conforme señalan los artículos 17 y 19.	Si la solicitud que tuviere fuese negativa, el artículo 13 del Reglamento a la Ley delimita que el titular de datos podrá presentar ante la Diprodap la denuncia correspondiente. El artículo 35 del mismo reglamento determina que será esta entidad la que realizará la investigación e instrucción del expediente por posibles infracciones. Iniciará la investigación e instrucción del expediente de conformidad al procedimiento administrativo establecido en los artículos del 36 al 52 del reglamento. Constan descritos en el capítulo VII, De las acciones de protección de datos personales.		El artículo 19 de la Ley 787-2012 señala que el informe de entrega de los datos o negándose motivadamente, se debe proporcionar dentro de los diez días hábiles siguientes a la recepción de la solicitud. Vencido el plazo sin que se haya rendido el informe, el interesado puede promover la acción de protección de datos personales prevista en esta ley.	Reglamento. Constan descritos en el capítulo VII, De las acciones de protección de datos personales, desde el artículo 47 al 52, el procedimiento pertinente que deberá llevarse a cabo en vía administrativa para la interposición de la acción de protección de datos personales, que deberá dirigirse ante la Dirección de Protección de Datos Personales, órgano encargado de conocer y resolverla.	
Panamá	SI. Art. 16 de la Ley 81 Artículo 16. El titular de datos personales o quien lo represente podrá solicitar su información a los responsables del tratamiento de datos, la cual deberá ser proporcionada en un plazo no mayor de diez días hábiles, a partir de la fecha de presentación de dicha solicitud. Sin perjuicio de las excepciones legales, el titular tendrá, además derecho a exigir que eliminen sus datos personales cuando su almacenamiento carezca de fundamento legal, cuando no hayan sido expresamente autorizados o cuando estuvieren caducos. El suministro de información, la modificación, bloqueo o la eliminación de los datos personales será absolutamente gratuito y deberá proporcionarse, a solicitud del titular de los datos o quien lo represente, constancia de la base de datos actualizada en lo	SI. Art. 16 de la Ley 81 (…) Sin perjuicio de las excepciones legales, el titular tendrá, además derecho a exigir que eliminen sus datos personales cuando su almacenamiento carezca de fundamento legal, cuando no hayan sido expresamente autorizados o cuando estuvieren caducos. (…) Artículo 17. LGPD Los datos deberán ser modificados cuando sean erróneos, inexactos, equívocos o incompletos dentro de un término de cinco días hábiles siguientes a la solicitud, de modificación, quien sea responsable de una base de datos regulada por esta Ley, podrá proceder a la eliminación, modificación o bloqueo de los datos personales sin necesidad de requerimientos del titular, cuando existan pruebas de inexactitud no pueda ser establecida o cuya vigencia y respecto de los cuales no	SI. Artículo 18. Si el responsable de la base de datos personales no se pronuncia sobre la solicitud del titular de datos personales dentro de los términos establecidos, el titular de los datos personales tendrá derecho a recurrir a la Autoridad Nacional de Transparencia y Acceso a la Información. En caso de sujetos regulados por leyes especiales, el ciudadano deberá acudir a la autoridad reguladora y, a falta de respuesta de esta, deberá recurrir a la Autoridad Nacional de Transparencia y Acceso a la Información. La Autoridad Nacional de Transparencia y Acceso a la Información está facultada para solicitar la información necesaria y efectuar verificaciones a fin de realizar las investigaciones administrativas relacionadas exclusivamente y en cada caso con la queja o denuncia	NO	SI. Art. 16 de la Ley 81 (…) cuando su almacenamiento carezca de fundamento legal, cuando no hayan sido expresamente autorizados o cuando estuvieren caducos.	Artículo 17. LGPD “(…) cuando existan pruebas de inexactitud no pueda ser establecida o cuya vigencia y respecto de los cuales no corresponda la cancelación (…)”	NO

	concerniente.	corresponda la cancelación. En este caso, serán bloqueados para acceso a terceros o para evitar su uso en otros fines que no hayan sido los expresamente autorizados. En todo caso, corresponderá a la Autoridad Nacional de Transparencia y Acceso a la Información, como autoridad competente, determinar cuándo un dato es inexacto o cuándo carece de fundamento legal, sin perjuicio de lo dispuesto en leyes especiales que regulen materias específicas.	presentada.			
Perú		Si el procedimiento por el que se opta es el de seguir la acción ante la Autoridad Nacional de Protección de Datos Personales, deberá sujetarse a lo dispuesto en los artículos 219 y siguientes de la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces.	La resolución de la Autoridad Nacional de Protección de Datos Personales agota la vía administrativa y habilita la imposición de las sanciones administrativas previstas en el artículo 39.		Art. 24, LPDP. El titular o el encargado del banco de datos personales que deniegue al titular de los mismos, total o parcialmente, el ejercicio de los derechos establecidos en esta ley, puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de *habeas data*.	El reglamento determina las instancias correspondientes. Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa.
República Dominicana		Art. 8, Ley 172-13. Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Toda persona tiene derecho a que sean rectificados, actualizados, y, cuando corresponda, suprimidos, los datos personales de los que sea titular y que estén incluidos en un banco de datos. El responsable del banco de datos, después de verificar y comprobar la pertinencia de la reclamación, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin, en el plazo máximo de diez (10) días hábiles de recibido el reclamo del titular de los datos o advertido el error o inexactitud.		Art. 17, Ley 172-13. Acción de hábeas data. Sin perjuicio de los mecanismos establecidos para el ejercicio de los derechos de los interesados, estos podrán ejercer la acción judicial de *habeas data* de conformidad con la Constitución y las leyes que rigen la materia.	Art. 8, Ley 172-13. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más requisitos la acción de protección de los datos personales o de *habeas data* prevista en esta ley.	Art. 17, Ley 172-13. La acción judicial de *habeas data* procederá para tomar conocimiento de la existencia de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados que se deriven de una relación comercial, laboral o contractual con una entidad pública o privada; o simplemente, para tomar conocimiento de los datos personales que se presuma que existen almacenados en archivos, registros o bancos de datos públicos o privados. En los casos en que se presuma inexactitud, la desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentre prohibido en la presente ley, para exigir su rectificación, supresión o actualización.

Uruguay	Art. 14, Ley 18.331. Derecho de acceso. Todo titular de datos personales, que previamente acredite su identificación con el documento de identidad o poder respectivo, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas. Este derecho de acceso solo podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico. Conforme el Decreto 414/009, los derechos de los titulares de los datos se ejercitarán por parte del titular o su representante, acreditando la identidad de ambos en su caso; se aplicará por extensión a las personas jurídicas en cuanto corresponda; en forma conjunta o independiente; exento de formalidades y en forma gratuita, mediante comunicación dirigida al responsable de la base de datos o tratamiento (art. 9°).	Art. 15. Toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular. El responsable de la base de datos o del tratamiento deberá proceder a realizar la rectificación, actualización, inclusión o supresión, mediante las operaciones necesarias a tal fin en un plazo máximo de cinco días hábiles de recibida la solicitud por el titular del dato o, en su caso, informar de las razones por las que estime no corresponde.	Art. 37. *Habeas data*. Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicas o privadas; y –en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización– a exigir su rectificación, inclusión, supresión o lo que entienda corresponder. Cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el juez apreciará el levantamiento del mismo en atención a las circunstancias del caso.	Art. 38. Procedencia y competencia. El titular de datos personales podrá entablar la acción de protección de datos personales o *habeas data*, contra todo responsable de una base de datos pública o privada, en los siguientes supuestos: A) Cuando quiera conocer sus datos personales que se encuentran registrados en una base de datos o similar y dicha información le haya sido denegada, o no le hubiese sido proporcionada por el responsable de la base de datos, en las oportunidades y plazos previstos por la ley. B) Cuando haya solicitado al responsable de la base de datos o tratamiento su rectificación, actualización, eliminación, inclusión o supresión y este no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la ley.

Fuente y elaboración: La autora (2018).

Como se analizó en la tabla 52, el *habeas data* en Latinoamérica puede ser reconocido en distintos niveles:

- Garantía constitucional (*habeas data*): Brasil (1988), Paraguay (1992), Perú (1993), Ecuador (1996), Venezuela (1999), Panamá (2002), Honduras (2003), República Dominicana (2010) y Nicaragua (2014).

- Otras acciones constitucionales: Se anota que en otros países no se reconoce el *habeas data*, pero en su lugar existen acciones constitucionales tradicionales como la tutela y el amparo que incluyen en ellas al *habeas data*. Colombia (1991) por medio de la acción de tutela constitucional, de Argentina mediante la acción de amparo (subtipo de amparo constitucional o *habeas data* constitucional) (1994) y de México a través de la Ley de Amparo, Reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos, cuyas últimas modificaciones corresponden al 17 de junio de 2016 que regula el Juicio de Amparo que procede sobre derechos constitucionales como el de protección de datos personales (art. 16 de la Constitución citada). Bolivia consagra en la Constitución la acción denominada de protección de la privacidad.

- Acción de protección de los datos personales o de *habeas data* legal (acción judicial): Argentina, Uruguay, Perú (agotamiento de vía procede la acción contencioso administrativa) y República Dominicana. Brasil reconoce el derecho de los interesados de ejercerse ante los tribunales, individual o colectivamente.

- Acciones directas contra el responsable de la base de datos: Países que basan su sistema de protección en la intimidad y la privacidad o con leyes sectoriales limitadas al ámbito público: El Salvador.

- Acciones directas contra el responsable de la base de datos contenidos en Leyes de Protección de Datos Personales: Argentina, Brasil, Colombia, Costa Rica, México, Nicaragua, Panamá, República Dominicana y Uruguay.

- Acciones ante autoridades administrativas competentes en protección de datos personales: Brasil, Costa Rica, Perú, Nicaragua, Panamá, México (tanto en la normativa de protección de datos personales para el sector privado como para el público). Jamaica y Puerto Rico (acción administrativa de privacidad).

- Acciones administrativas en países que basan su sistema de protección en la intimidad y la privacidad o con leyes sectoriales limitadas al ámbito público o específicos: El Salvador y Chile.

- No se contemplan acciones administrativas (sistema de protección en la intimidad y la privacidad o con leyes sectoriales limitadas al ámbito público o específicos): Bolivia, Paraguay, Honduras y Venezuela. Ecuador, aunque reconoce el derecho a la protección de datos personales, no existe normativa específica. Guatemala normativa aplicable solo al ámbito público. Panamá: no consta en la normativa constitucional ni legal panameña referencia a procedimiento administrativo; la acción aplicable es la de *habeas data* que es de carácter constitucional y desarrollada en ley específica, Ley 6 de 2002.

1.5.7 Habeas data

Para entender cómo se configura el *habeas data* se debe señalar que:

> Etimológicamente *hábeas data* significa "conservar o guardar los datos", o con mayor propiedad como lo señala Morogana Díaz citando a Otón Sidow "que tengas los registros, lo datos", habiéndose puesto de resalto su similitud con el *hábeas corpus*. Se ha hecho notar que a semejanza de este último instituto, en el que se impetra la presentación del "cuerpo" del privado de su libertad para investigar los motivos de la misma, y en su caso disponer la cesación de ese estado, en el *hábeas data* se requiere se presenten los datos para la verificación de su exactitud, actualidad, etc., a efecto de exigir si correspondiere, su inmediata rectificación, actualización, sometimiento a confidencialidad, reserva, etc.[1536]

Ekmekdjian y Pizzolo respecto del origen etimológico de los términos *habeas data* señalan que:

> El hábeas data no tiene añeja o rancia prosapia. Es una de las garantías constitucionales más modernas, aunque se la denomine mitad en latín y mitad en inglés. En efecto, su nombre se ha tomado parcialmente del antiguo instituto del *hábeas corpus*, en el cual el primer vocablo significa "conserva o guarda tú…", y del inglés "*data*". En síntesis, en una traducción literal sería "conserva o guarda tus datos".[1537]

El *habeas data* es una garantía constitucional por la cual los ciudadanos tienen derecho a verificar que los datos que se encuentran en los ficheros de terceros se encuentren actualizados, completos, correctos, y que de no ser así puedan ejercitar los derechos de rectificación, actualización o cancelación; es decir, un derecho de control sobre sus datos, con lo cual también se protegen otros derechos, tales como la honra, la buena reputación, la identidad y también el derecho a la información. Por eso, se afirma que fue constituido para conseguir el amparo prometido a la "generosa tutela judicial prometida a los derechos derivados de la vida privada (intimidad y privacidad)".[1538]

De la clasificación que ha realizado la mayoría de la doctrina y de la evidencia de la normativa latinoamericana, se puede concluir que los tipos de *habeas data* que protegen en las distintas normativas constitucionales son:

a) *Habeas data* informativo.
b) *Habeas data* aditivo actualizador.
c) *Habeas data* rectificador o correctivo.
d) *Habeas data* exclutorio o cancelatorio.
e) *Habeas data* reparador.

Resta aclarar el por qué el *habeas data* goza de la doble calidad de constituirse una garantía constitucional y un derecho fundamental. Al respecto, debe señalarse la naturaleza jurídica de la garantía constitucional por la cual:

[1536] G. PEYRANO, *Régimen legal de los datos personales y hábeas data* (Buenos Aires: Lexis Nexis, Depalma, 2002), 284.
[1537] M. A. EKMEKDJIAN; C. PIZZOLO, *Hábeas data: el derecho a la intimidad frente a la revolución informática* (Buenos Aires: Ediciones Depalma, 1996), 1.
[1538] GOZAÍNI, *Hábeas Data*, 56.

> [...] se encuentra destinada a la protección de derechos por disposición de la misma Constitución Nacional, se trata de una garantía. En atención a su carácter de acción judicial, reviste un obvio carácter procesal. Por tanto se trata de una "garantía de carácter constitucional" correspondiente a la órbita del derecho procesal constitucional. Atento a su afinidad con el amparo y a las características de urgencia y expeditividad que ambos institutos comparte, se encuentra dentro del espectro de los denominados "proceso urgentes", los cuales "se tipifican cuando concurren situaciones que exigen una particularmente presta respuesta y solución jurisdiccional".[1539]

El *habeas data* es una garantía y un derecho al mismo tiempo que faculta a su titular, a través de un mecanismo constitucional, a controlar la calidad de los datos, "corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su posible transmisión"[1540]

El *habeas data* al ser una garantía de rango constitucional, si bien necesita un desarrollo legal, este es de índole complementario, pues lo significativo de un derecho-garantía es su aplicación directa y la posibilidad de la exigencia efectiva del derecho fundamental que consagra, ante un juez de primer nivel, quien solicita al funcionario que dispone de la información, el presentarla, explicar el uso que se está dando y el propósito de la entidad que tiene esa información; es decir, prescindir de acudir a entidades especializadas para iniciar reclamos administrativos, que eventualmente terminarán en la función judicial.

La mayoría de Constituciones, entre las que consta la ecuatoriana,[1541] incluyen el *habeas data* dentro del capítulo de las acciones procesales constitucionales; y al momento de establecer el texto señalan que el *habeas data* también es un derecho sobre todo cuando se describen en su contenido derechos de acceso, rectificación, eliminación, entre otros.
Ahora bien, Ximena Puente de la Mora, respecto de lo expresado por Palazzi, señala que no coincide:

> [...] en el sentido de que el habeas data representa apenas un intento dirigido a corregir distorsiones extremas del proceso comunicativo informático, ya que de un lado reduce la invisibilidad de los gestores o titulares de los bancos de datos porque los hace sujetos de una responsabilidad clara ante el titular de los mismos, y por el otro lado, permite a las personas en cierta medida adquirir conciencia de la transparencia externa e incluso de la importancia que tiene su propia información personal. Sin embargo, no coincide con el autor en que el habeas data "representa un intento 'incipiente y tímido' puesto que para accionar [...] se requiere el funcionamiento del aparato jurisdiccional establecido por los países (en su mayoría latinoamericanos); en todo caso, estaríamos hablando de la mejora de las instituciones judiciales y no de que representara una falla en la estructuración del mismo habeas data.[1542]

Coincidimos con Puente en la afirmación de que el *habeas data* no debe ser minimizado, sobre todo, porque como garantía constitucional tiene una funcionalidad

---

[1539] PEYRANO, *Régimen legal*, 285.
[1540] M. A. EKMEKDJIAN; C. PIZZOLO, *Hábeas data: el derecho a la intimidad frente a la revolución informática* (Buenos Aires: Ediciones Depalma, 1996), 1.
[1541] "Art. 94.- Toda persona tendrá *derecho* a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito."
[1542] X. PUENTE DE LA MORA, *Latinoamérica ante la tendencia europea y norteamericana en la regulación del flujo transfronterizo de datos personales*, *Revista de Derecho Informático*, n.º. 100 (2006).

propia de carácter correctivo; es decir, ante la existencia de un derecho vulnerado, el titular del dato puede reclamarlo. Se concibe como un sistema de cierre o de clausura para evitar un posible daño o cuando este ya se ha producido reparar las posibles transgresiones o impedir que estas sucedan.

Esta funcionalidad posterior es la que puede significar para Palazzi un intento tímido, ya que como se ha podido evidenciar, no es suficiente la implementación de esta garantía de aplicación post. Sino que es indispensable para una adecuada protección de carácter integral que exista normativa que desarrolle la protección del derecho, no solo en el ámbito constitucional sino en el administrativo, pero aún más desde una perspectiva preventiva que permita controlar a los responsables de ficheros, incluyendo al Estado, para evitar que los daños a los datos personales se produzcan.

Es propia del sistema latinoamericano la protección de la persona desde la perspectiva de la intimidad y la privacidad, mediante la consagración de una garantía constitucional de *habeas data*. Su reconocimiento inicial estuvo en Brasil en el año 1988, así como la mayoría de Constituciones de la región como la de Paraguay en 1992, Perú en 1993, Ecuador en 1996, Venezuela en 1999, Panamá en 2002, Honduras en 2003, República Dominicana en 2010 y Nicaragua en el 2014.

Otros países optaron por otras garantías constitucionales como la tutela en el caso de Colombia en el año 1991. Argentina lo hizo mediante el subtipo de amparo constitucional o *habeas data* constitucional en 1994. Bolivia consagró inicialmente al *habeas data* para, posteriormente, consagrar la acción denominada de protección de la privacidad.

Lamentablemente, de los países analizados El Salvador, Bolivia, Brasil, Chile, Honduras, Paraguay y Venezuela mantienen una perspectiva limitada de protección atada a la intimidad; por tanto, en aquellos países la acción constitucional se encuentra acotada a este derecho fundamental.

Por su parte, los otros países de la región: Argentina, Colombia, Costa Rica, Ecuador, Guatemala, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay, al reconocer a nivel constitucional o legal el derecho a la protección de datos personales, permitieron que el *habeas data* no solo proteja la intimidad de los individuos, sino otros derechos fundamentales.

Además, en Argentina, Colombia, Costa Rica, México, Nicaragua, Perú, República Dominicana y Uruguay se optó además por un desarrollo legal que permitiera desarrollar no solo un sistema reactivo de garantía, sino un preventivo que establece los principios y derechos inherentes a la protección de datos personales, de tal manera que el daño al individuo se evite y no solo se active el sistema de protección estatal cuando la transgresión ya se ha producido como ocurre con el *habeas data*. Aunque si existen en muchos países otras garantías constitucionales que prevén la posibilidad de anticiparse al daño y evitarlo mediante medidas cautelares. Sin embargo, en el caso de los datos personales y su régimen es muy difícil a nivel fáctico avizorar posibles afectaciones en las que estas medidas constitucionales previas puedan evitar la violación del derecho.

Desde la perspectiva de la intimidad, se colige lo siguiente:

Tabla 53

País	*Habeas data*	Otra acción	Sujeto activo	Sujeto pasivo u obligado	Derechos tutelados por el *habeas data*	Procedencia *habeas data*	Procedimiento de *habeas data*
El Salvador	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Bolivia		**Acción de protección de privacidad.** La Constitución de la República de Bolivia de 2009 abroga la Constitución Política del Estado de 1967 y sus reformas posteriores (art. 130).	Toda persona individual o colectiva	**Quien está a cargo.** La Constitución señala que la acción procede contra quien está a cargo de los archivos o bancos de datos sean estos públicos o privados (art. 130).	**Intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación.** Artículo 130.	Art. 130. I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad. II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.	El artículo 131 de la Constitución de 2009 señala que el procedimiento de la Acción de Protección de Privacidad será el mismo previsto para la acción de amparo constitucional. Esta decisión podrá elevarse, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución.
Chile	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Honduras	***Habeas data***. Mediante Decreto 243/2003 se incluye en el título IV, denominado de las garantías constitucionales, el capítulo I, *habeas corpus*, *habeas data* y el amparo. Otra reforma a la Constitución hondureña mediante Decreto 381-2005, 20 de enero del 2006, publicado en el Diario Oficial La Gaceta 30,920, 4 de febrero del 2006, que respecto del título IV, denominado de las garantías constitucionales, capítulo I, *habeas corpus*, *habeas data* y el amparo que determina el nuevo contenido del artículo 182.		**Persona.** Es la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados (art. 182).	**Responsable.** Son responsables de las bases de datos públicas o privadas donde se encuentren almacenados los datos personales (art. 182).	**Honor, la intimidad personal, familiar y la propia imagen.** Solo protegen datos personales que produzcan daño y que una vez activados los mecanismos jurisdiccionales expresamente se determina la obligación ineludible de proceder de inmediato para hacer cesar la violación a la libertad, la seguridad personal, el honor, la intimidad personal, familiar o la propia imagen. No se ha concebido la autodeterminación informativa como elementos esenciales dentro del derecho a la protección de datos personales.	Según el artículo 182 de la Constitución hondureña procede el *habeas data* para obtener acceso a la información; impedir su transmisión o divulgación; rectificar datos; actualizar información, exigir confidencialidad y su eliminación, pero señala expresamente que los datos deben ser inexactos o erróneos o la información falsa; así como que produzcan daño al honor, a la intimidad personal, familiar y a la propia imagen.	Es competente para conocer el *habeas data* la Sala de lo Constitucional de la Corte Suprema de Justicia. Además, como forma de evitar dilaciones e ineficacia de la administración de justicia se determina que los titulares de los órganos jurisdiccionales no podrán desechar estas acciones constitucionales y tienen la obligación ineludible de proceder de inmediato para hacer cesar la violación a la libertad, la seguridad personal, el honor, la intimidad personal, familiar o la propia imagen.
Paraguay	***Habeas data*** El artículo135 de la Constitución del Paraguay.- Del Hábeas Data.		Según el artículo 135 de la Constitución, sobre el *habeas data,* "Toda persona…"	Todos los que afecten el derecho.	La norma constitucional que recoge al *habeas data* no señala de forma expresa qué derechos se tutela bajo su órbita, pero conforme señala la jurisprudencia paraguaya, la acción de *habeas data* como garantía constitucional protege a la	Art. 135, Constitución. Del Hábeas Data. "Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se	En el artículo 135 de la Constitución del Paraguay no se especifica cuál sería la autoridad competente para entender la acción de *habeas data*, solo menciona la frase "podrá solicitar ante el magistrado

					intimidad personal y familiar por intermedio de ella a la imagen, a la honra, la buena reputación, la voz e imagen propias, a la dignidad, al honor y a la identidad personal, el derecho de rectificación en medios de comunicación social e incluso combate la discriminación. Siempre desde la perspectiva de ponderación de derechos entre la intimidad y el derecho de información.	haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegitimamente sus derechos".	competente".
Venezuela	***Habeas data*** Artículo 28 de la Constitución de Venezuela.	**Toda persona, incluidas comunidades o grupos de interés con la condición básica de que contengan información cuyo conocimiento sea de su interés y sujeto coadyuvante el Defensor del Pueblo.** Artículo 28 de la Constitución de Venezuela. Toda persona tiene derecho... Será sujeto activo coadyuvante, el Defensor del Pueblo de conformidad con el artículo 281 de la Constitución que le establece la facultad de interponer acción de *habeas data*. Por ello es que, entre las facultades de la Defensoría del Pueblo consta la de presentar acción de *habeas data* en beneficios de niños, niñas y adolescentes (art. 170-A, lit. h), Ley Orgánica para la Protección de Niños, Niñas y Adolescentes, publicada en la Gaceta Oficial 5.859, 10 de diciembre de 2007.	**Quienes tienen a su cargo registros oficiales o privados.** Legitimados pasivos de la garantía de *habeas data* serán aquellos que tienen a su cargo los registros oficiales o privados. Y por disposición expresa de carácter constitucional no pueden ser sujetos pasivos aquellos que tengan información en virtud del secreto de las fuentes periodísticas o del ejercicio de aquellas profesiones determinadas en la ley (art. 28, Constitución).	**Honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas.** La norma constitucional, artículo 28, no menciona expresamente qué derechos son los tutelados por el *habeas data*, pero al ser una garantía constitucional protege en esencia los derechos descritos en el artículo 60: honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas.	Art. 28, Constitución. "Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley".	Se establece un procedimiento para la garantía constitucional de *habeas data* mediante una jurisprudencia de aplicación obligatoria dictada por la Sala Constitucional del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela, mediante la resolución 1511/2009.

Fuente y elaboración: La autora (2018).

a) Respecto del derecho a la protección de datos personales:

Tabla 54

País	Garantía constitucional	Garantía legal	Otra garantía	Sujeto activo	Sujeto pasivo	Derechos tutelados por el *habeas data*	Procedencia *habeas data*	Procedimiento y recurso de alzada
Argentina	NO.	NO.	**Subtipo de amparo.** Artículo 43, Ley 16.986, Ley de Acción de Amparo de 1966. "Toda persona podrá interponer esta	**Persona natural y jurídica.** La norma constitucional señala expresamente a toda persona, esto incluye a persona natural y a persona jurídica respecto de	**Responsables.** El artículo 43 de la Carta Magna argentina señala que deberá accionarse contra los responsables de los registros o bancos de datos	**Intimidad, privacidad, honor y protección de datos personales.** Como en el presente caso se trata de un subtipo de la acción de amparo, la norma constitucional al	Como este *habeas data* constitucional es un subtipo de la acción de amparo, le es pertinente aquellos criterios de procedencia que definen a este tipo de acciones, esto es que toda persona	**Agotada la vía administrativa.** La Ley 16.986 señala en el artículo 2 que la acción de amparo no será admisible cuando: a) Existan recursos o

			acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".	este derecho en específico, toda vez que es de aquellos que pueden ser invocados por un ente inmaterial, conforme el artículo 43 de la Constitución. Asimismo, el artículo 5 de la Ley de Acción de Amparo señala que podrá deducirse por toda persona individual o jurídica, por sí o por apoderados, por las asociaciones que sin revestir el carácter de personas jurídicas justificaren, mediante la exhibición de sus estatutos, que no contrarían una finalidad de bien público.	públicos o de los privados destinados a proveer informes. La Ley 16.986 señala en el artículo 1 que la acción de amparo se dirigirá en contra de la autoridad pública que, en forma actual o inminente, lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, los derechos o garantías explícita o implícitamente reconocidas por la Constitución nacional.	ser una garantía protege los derechos contemplados en los artículos 18 y 19 de la Carta Magna, esto es intimidad, privacidad, honor. Pero adicionalmente, por referirse el contenido del artículo 43 de la Constitución a que esta acción faculta a su titular a tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, se entiende que también está tutelado el derecho a la protección de datos personales, aunque en una versión limitada que apuntala al acceso más que un derecho de control sobre los datos personales de un titular.	natural o jurídica puede interponerlo cuando no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley (art. 43, Constitución argentina). Además, la necesidad de que la información personal conste en registros o bancos de datos públicos, o los privados destinados a proveer informes. Añadiendo que solo procede cuando los datos personales sean falsos o le generen a su titular discriminación (art. 43 Constitución argentina).	remedios judiciales o administrativos que permitan obtener la protección del derecho o garantía constitucional de que se trate; b) El acto impugnado emanara de un órgano del Poder Judicial. Respecto del procedimiento, es aplicable el establecido en la Ley 16.986, Ley de Acción de Amparo. Será competente para conocer de la acción de amparo el juez de Primera Instancia con jurisdicción en el lugar en que el acto se exteriorice o tuviere o pudiere tener efecto (art. 4).
Brasil	***SI, Habeas data***. Artículo 5 de la Constitución de la República Federativa de Brasil de 1988.	NO	**NO**	Art. 5, Constitución brasileña. "Todos son iguales ante la ley, sin distinción de cualquier naturaleza, garantizándose a los brasileños y a los extranjeros residentes en el País la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la prioridad..."	De acuerdo con lo señalado en el artículo 5 de la norma constitucional brasileña, el *habeas data* solo tiene como sujeto pasivo a las entidades gubernamentales o de carácter público que almacenan datos catastrales. Esto porque esta norma constitucional no ha sido modificada y en consecuencia no se integran aún a la esfera de protección del *habeas data*, las bases privadas.	No existe alusión a los derechos que son tutelados mediante el *habeas data*, pero por la simple lectura del artículo 5 de la Constitución se infiere que protege a la autodeterminación informativa. Ya que, conforme señala el citado artículo, se concederá *habeas data* para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público y para la rectificación de datos.	Art. 5 de la Constitución de la República Federativa de Brasil de 1988, LXXI. Se concederá hábeas data: a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo.	Art. 5, Constitución de la República Federativa de Brasil de 1988, LXXVI. Son gratuitas las acciones de "hábeas corpus" y "hábeas data" y, en la forma de la ley, los actos necesarios al ejercicio de la ciudadanía.
Colombia	NO. El *habeas data* en Colombia no es la garantía constitucional sino el derecho en sí mismo; por eso, la acción constitucional prevista en la Constitución colombiana para la protección de estos es la acción de tutela.	NO.	**Acción de tutela.** Art. 86, Constitución. "Toda persona tendrá acción de tutela para reclamar ante los jueces, en todo momento y lugar, mediante un procedimiento preferente y sumario, por sí misma o por quien actúe a su nombre, la protección inmediata de sus derechos constitucionales fundamentales, cuando quiera que éstos resulten vulnerados o amenazados	**Todas las personas.** El artículo 86 de la Constitución señala que serán sujetos activos de la acción de tutela de amparo todas las personas, por sí mismas o por quien actúe a su nombre. Por cuanto son titulares del derecho personas naturales y jurídicas, se comprende que para garantizarlos y solicitar su efectiva tutela lo son también de la acción de amparo.	El artículo 86 de la Constitución señala que "La ley establecerá los casos en los que la acción de tutela procede contra particulares encargados de la prestación de un servicio público o cuya conducta afecte grave y directamente el interés colectivo, o respecto de quienes el solicitante se halle en estado de subordinación o indefensión".	**Todos los derechos fundamentales** "Artículo 86. Toda persona tendrá acción de tutela para reclamar ante los jueces, en todo momento y lugar, mediante un procedimiento preferente y sumario, por sí misma o por quien actúe a su nombre, la protección inmediata de sus derechos constitucionales fundamentales, cuando quiera que éstos resulten vulnerados o amenazados por la acción o la omisión de cualquier autoridad	El artículo 86 de la Constitución señala que "Esta acción sólo procederá cuando el afectado no disponga de otro medio de defensa judicial, salvo que aquella se utilice como mecanismo transitorio para evitar un perjuicio irremediable. En ningún caso podrán transcurrir más de diez días entre la solicitud de tutela y su resolución".	El artículo 86 de la Constitución señala que "La protección consistirá en una orden para que aquél respecto de quien se solicita la tutela, actúe o se abstenga de hacerlo. El fallo, que será de inmediato cumplimiento, podrá impugnarse ante el juez competente y, en todo caso, éste lo remitirá a la Corte Constitucional para su eventual revisión". El titular o causahabiente antes de acudir y presentar reclamo ante la Superintendencia de

			por la acción o la omisión de cualquier autoridad pública".			pública.		Industria y Comercio debe elevar previamente queja ante el responsable o el encargado del tratamiento.
Costa Rica	NO.	NO.	**Recurso de amparo.** El artículo 13 de la Ley 8968 determina que pese a la vía administrativa, existen garantías jurisdiccionales generales o específicas que han sido establecidas en salvaguarda del derecho a la protección de datos personales, entre ellas la acción de amparo contenida en la Ley 7135 del 11/10/1989, Ley de la Jurisdicción Constitucional, reformada el 31/10/2011.	**Cualquier persona.** El artículo 33 de la Ley 7135 determina que cualquier persona podrá interponer el recurso de amparo.	**Servidor o el titular del órgano.** El artículo 34 de la Ley 7135 señala que el recurso de amparo podrá dirigirse contra el servidor o el titular del órgano que aparezca como presunto autor del agravio. Si uno u otro hubiesen actuado en cumplimiento de órdenes o instrucciones impartidas por un superior, o con su autorización o aprobación, se tendrá por establecido el amparo contra ambos, sin perjuicio de lo que se decida en sentencia. De ignorarse la identidad del servidor, el recurso se tendrá por establecido contra el jerarca.	**Derechos de intimidad, honor y protección de datos personales.** El artículo 29 de la Ley 7135 determina que el recurso de amparo garantiza los derechos y libertades fundamentales, salvo los protegidos por el de *habeas corpus*. La Sala Constitucional reconoce el derecho a la protección de datos personales resoluciones de amparo constantes en las sentencias 4154-97, 7175-97, 4347-99 y 5802-99, analizadas previamente.	El artículo 29 de la Ley 7135 determina que el recurso de amparo procede contra toda disposición, acuerdo o resolución y, en general, contra toda acción, omisión o simple actuación material no fundada en un acto administrativo eficaz, de los servidores y órganos públicos, que haya violado, viole o amenace violar cualquiera de aquellos derechos.	Según el artículo 39, la tramitación del recurso estará a cargo del Presidente de la Sala o del magistrado a quien este designe y se sustanciará en forma privilegiada, para lo cual se pospondrá cualquier asunto de naturaleza diferente, salvo el de *habeas corpus*. Los plazos son perentorios e improrrogables, sin perjuicio de lo dispuesto en el artículo 47.
Ecuador	**Acción de hábeas data.** Art. 92, Constitución. "Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos".	NO.	NO.	**Persona natural, jurídica y comunidad pueblo y nacionalidad.** Persona natural. Se analizará cada caso particular respecto de persona jurídica, comunidad, pueblo, nacionalidad y colectivo. Sentencia001-2014-PJO-CC. Registro Oficial Suplemento 281, 3 julio de 2014. Sentencia vinculante. Art. 92, Constitución. "Toda persona, por sus propios derechos o como representante legitimado para el efecto…"	**Quien recolecte.** Art. 92, Constitución. Toda persona que recolecte, archive procese, distribuya o difunda datos o información.	**Protege a la intimidad, al buen nombre, el honor, la imagen y la propia voz, derecho a la protección de datos personales.** **Derecho de rectificación en medios de comunicación social.** Art. 92, Constitución; Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional de 2009. "Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de	Procede *habeas data* cuando se niegue el acceso. Cuando se niegue la solicitud de actualización, rectificación eliminación o anulación de datos erróneos o que afecten sus derechos. Cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de juez competente. Art. 92 de la Constitución de la República del Ecuador; art. 52 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional de 2009.	Art. 52, Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional de 2009. La persona titular de los datos podrá solicitar al responsable si costó el acceso, la actualización, rectificación, eliminación o anulación. Si la solicitud no fuere atendida podrá acudirse al juez de primera instancia que actúa como juez constitucional a través de *habeas data*. La sentencia de primera instancia podrá ser apelada ante la Corte Provincial. Las sentencias ejecutoriadas serán remitidas a la Corte Constitucional, la que por medio de la Sala de selección escogerá aquellas que permiten desarrollar el sistema de precedentes jurisprudenciales.

						seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados".		
Guatemala	NO.	Art. 9, Decreto 57-2008, 23/09/2008, Ley de Acceso a la Información Pública. "Definiciones. Para los efectos de la presente ley, se entiende por: [...] 4. Habeas data: Es la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización".	NO.	**Persona individual o jurídica, pública o privada.** Arts. 2 y 5, Decreto 57-2008, 23/09/2008, Ley de Acceso a la Información Pública. Artículo 5. Sujeto activo. Es toda persona individual o jurídica, pública o privada, que tiene derecho a solicitar, tener acceso y obtener la información pública que hubiere solicitado conforme lo establecido en esta ley.	Art. 4, Decreto 57-2008, 23/09/2008, Ley de Acceso a la Información Pública. Artículo 6. Sujetos obligados. Es toda persona individual o jurídica, pública o privada, nacional o internacional de cualquier naturaleza, institución o entidad del Estado, organismo, órgano, entidad, dependencia, institución y cualquier otro que maneje, administre o ejecute recursos públicos, bienes del Estado, o actos de la administración pública en general, que está obligado a proporcionar la información pública que se le solicite, dentro de los que se incluye el siguiente listado, que es enunciativo y no limitativo.	**Protección de datos personales.** Según el artículo 9 de la Ley de Acceso a la información Pública, el *habeas data* es la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización. Los datos impersonales no identificables, como aquellos de carácter demográfico recolectados para mantener estadísticas, no se sujetan al régimen de *habeas data* o protección de datos personales de la presente ley.	El artículo 34 señala que en el caso de presentar el recurso de *habeas data* con la finalidad de modificar los datos registrados, este procede cuando es solicitado por los titulares o sus representantes legales, previa acreditación de esta condición: en el documento se deben indicar las modificaciones que desea realizar y aportar la documentación que motive su petición.	**Sin necesidad de acto negativo previo.** Como se trata de una acción directa, es decir que se ejerce frente al propio Estado, opera sin necesidad de acto negativo previo. No necesita que el responsable niegue el acceso, ni la solicitud de actualización, rectificación eliminación o anulación de datos erróneos o que afecten sus derechos. **Recurso de revisión.** Decreto 57-2008, 23/09/2008, Ley de Acceso a la Información Pública, art. 35. Denegación expresa. Contra la negativa de entregar o corregir datos personales, procederá la interposición del recurso de revisión previsto en esta ley.
México	NO.	NO.	**Juicio de Amparo** La Ley de Amparo, Reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos, cuyas últimas modificaciones corresponden al 17 de junio de 2016; regula el Juicio de Amparo.	**Persona natural o jurídica.** Arts. 103 y 107. El quejoso, persona natural o jurídica, por sí, por su representante legal o por su apoderado (art. 6), que aduce ser titular de un derecho subjetivo o de un interés legítimo individual o colectivo, siempre que alegue que la norma, acto u omisión reclamados violan los derechos constitucionales y con ello se produzca una afectación real y actual a su esfera jurídica. El menor de edad, persona con discapacidad o mayor sujeto a interdicción pedirá amparo por sí o por cualquier persona en su nombre sin la intervención de legítimo representante cuando este se halle ausente, se ignore	**Autoridad responsable o particular que realicen actos equivalentes.** La autoridad responsable, que es aquella que dicta, ordena, ejecuta o trata de ejecutar el acto que crea, modifica o extingue situaciones jurídicas en forma unilateral y obligatoria; u omita el acto que de realizarse crearía, modificaría o extinguiría dichas situaciones jurídicas, independientemente de su naturaleza formal. Para los efectos de esta ley, los particulares tendrán la calidad de autoridad responsable cuando realicen actos equivalentes a los de autoridad, que afecten derechos en los términos de esta fracción, y cuyas funciones estén determinadas por una norma general (art. 5). En el caso, las	**Derechos humanos.** Derechos humanos reconocidos otorgados para su protección por la Constitución Política de los Estados Unidos Mexicanos, así como por los tratados internacionales de los que el Estado mexicano sea parte (art. 1), entre ellos los constantes en los artículos 6 y 16.	El juicio de amparo tiene por objeto resolver toda controversia que se suscite por normas generales, actos u omisiones de autoridad que violen los derechos humanos reconocidos y las garantías otorgadas para su protección por la Constitución Política de los Estados Unidos Mexicanos, así como por los tratados internacionales de los que el Estado Mexicano sea parte (art. 1). Es precisamente aplicable a sujetos obligados que incumplan sus obligaciones de garantía y respeto del derecho a la protección de datos personales. La norma señala que mediante el amparo también puede protegerse a las personas frente a normas generales, actos u omisiones por parte de particulares en los casos	En este sentido, las resoluciones del Instituto y de los organismos garantes respecto de recursos de revisión serán vinculantes, definitivas e inatacables para los responsables. Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación mediante el Juicio de Amparo (art. 115). En el mismo sentido respecto del recurso de inconformidad (arts. 116 y 129).

				quién sea, esté impedido o se negare a promoverlo (art. 8) y el representante de la sucesión (art. 16).	negativas de acceso, rectificación, cancelación u oposición no justificada conforme la ley determinan actos susceptibles de juicio de amparo.		señalados en la presente ley.	
Nicaragua	El artículo de la Constitución de Nicaragua, reformada en el 2014, dispone que "las personas cuyos derechos constitucionales hayan sido violados o estén en peligro de serlo, pueden interponer el recurso de exhibición personal, de amparo, o de hábeas data, según el caso y de acuerdo con la Ley de Justicia Constitucional". Según el artículo 190, se establecen también los siguientes recursos y mecanismos de control constitucional: 1. El Recurso de Habeas Data como garantía de tutela de datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos, de naturaleza pública o privada, cuya publicidad constituya invasión a la privacidad personal y tenga relevancia con el tratamiento de datos sensibles de las personas en su ámbito íntimo y familiar. El Recurso de Habeas Data procede a favor de toda persona para saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales y su publicidad indebida.	El artículo 84, Ley 831, Ley de Reforma y Adiciones a la Ley 49, Ley de Amparo, aprobada el 30 de enero del 2013, señala el recurso de *habeas data*.	NO.	**Personas naturales y jurídicas.** El artículo 45 de la Constitución de Nicaragua, reformada en el 2014, dispone que "las personas cuyos derechos constitucionales hayan sido violados o estén en peligro de serlo, pueden interponer el recurso de exhibición personal, de amparo, o de hábeas data, según el caso y de acuerdo con la Ley de Justicia Constitucional". El artículo 84 de la Ley 831, Ley de Reforma y Adiciones a la Ley 49 Ley de Amparo de 2013, señala que el recurso de *habeas* data podrá ser interpuesto por las siguientes personas: a. Persona natural afectada; b. Tutores y sucesores o apoderados de las personas naturales afectadas; c. Personas jurídicas afectadas por medio de representantes legales o apoderados designados para tales efectos	**Responsables.** El artículo 84 quater expresa referencia a que el recurso de *habeas data* se dirige contra los responsables y cualquier otra persona que hubiere hecho uso indebido de ficheros de datos públicos o privados, o ambos.	**Vida privada y familiar, a la honra y reputación y a la autodeterminación informativa.** El artículo 5 bis. de la Ley de Amparo reformada señala que el recurso de *habeas data* se crea como garantía de tutela de datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos, de naturaleza pública o privada, cuya publicidad constituya una invasión a la privacidad personal y tenga relevancia con el tratamiento de datos sensibles de las personas en su ámbito íntimo y familiar. El artículo 84 bis. de la Ley de Amparo establece el recurso de *habeas data* procede en defensa de los derechos constitucionales reconocidos en el artículo 26, numerales 1, 3 y 4 de la Constitución Política de la República de Nicaragua; es decir, los derechos a la vida privada y familiar, a la honra y reputación y a la autodeterminación informativa. Asimismo, el artículo 190 de la Constitución cuando menciona *habeas data* expresamente señala que el ámbito de protección incluye la autodeterminación informativa.	El artículo 84 bis de la Ley de Amparo reformada en 2013 señala que el recurso de *habeas data* procede para: a) acceder a información personal; b) exigir la oposición, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación y actualización cuando se presuma la falsedad, inexactitud, desactualización, omisión total o parcial o la ilicitud de la información de que se trate; c) exigir la oposición, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación y actualización de cualquier publicidad de datos personales sensibles que lesionen los derechos constitucionales.	**Agotada la vía administrativa.** La Ley 831, Ley de Reforma y Adiciones a la Ley 49, Ley de Amparo, aprobada el 30 de enero del 2013 determina que para interponer el Recurso de Habeas Data se requiere que la persona legitimada procesalmente para ello, previamente haya agotado la vía administrativa contemplada en la Ley 787, Ley de Protección de Datos Personales, publicada en La Gaceta, Diario Oficial 61, 29 de marzo del 2012, y su Reglamento, Decreto 36-2012, publicado en La Gaceta, Diario Oficial 200, 19 de octubre del 2012. El recurso se interpondrá dentro de los treinta días (30) días posteriores a la notificación de la autoridad administrativa competente en materia de protección de datos personales; se considera también agotada la vía administrativa si dentro del plazo de los treinta días (30) días la autoridad administrativa no emite su resolución correspondiente.
Panamá	La Gaceta Oficial 25176 de 2004 reconoce, por primera vez, el derecho de acceso a la información pública, el acceso a información de carácter personal, y la acción constitucional de *habeas data*.	NO.	NO.	**Todas las personas.** Conforme señala el artículo 44 de la Constitución, que coincide con el artículo 17 de la Ley 6 que desarrolla la acción de *habeas data*, los titulares y legitimada para promover esta acción son todas las personas.	**Quienes recaban datos.** El artículo 44 de la Constitución señala, de manera indirecta e incluso confusa, que los sujetos pasivos de la acción de *habeas data* son los que recaban en bancos de datos o registros oficiales o particulares datos personales, cuando estos últimos traten de empresas que prestan un servicio al público o se dediquen a suministrar información.	**Acceso a la información y protección de datos personales.** El artículo 44 de la Constitución establece como derechos tutelados por el *habeas data* al derecho de acceso a la información pública o de acceso libre; así como también se podrá solicitar que se corrija, actualice, rectifique, suprima o se mantenga en confidencialidad la información o datos que tengan carácter personal. Es de naturaleza mixta puesto que el *habeas data* se	El artículo 44 de la Constitución, únicamente realiza una vaga determinación relativa a que la procedencia de la acción constitucional se realizará de conformidad con lo establecido en la propia Constitución.	No consta en la norma constitucional panameña referencia al procedimiento de *habeas data*, sino que está descrita en la Ley 6 de 2002. En el artículo 18 de la ley en mención consta que el *habeas data* será de competencia de los Tribunales Superiores que conocen de la acción de amparo de garantías constitucionales, cuando el funcionario titular o responsable de registro, archivo o banco de datos, tenga mando y

						considera tanto para datos públicos, como para datos personales, cuando en otras legislaciones se establece una acción constitucional propia denominada acceso a la información pública y otra la de *habeas data* circunscrita exclusivamente a datos personales.		jurisdicción en el nivel municipal o provincial. Cuando el titular o responsable del registro, archivo o banco de datos tenga mando y jurisdicción en dos o más provincias o en toda la república, será de competencia del Pleno de la Corte Suprema de Justicia.
Perú	En la Carta Política peruana consta el artículo 200 sobre las garantías constitucionales. Son garantías constitucionales 3) La acción de hábeas data, que procede contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5) y 6) de la Constitución. Ley 28237, 31 de mayo de 2004, Código Procesal Constitucional.	NO.	NO.	**Persona natural y jurídica.** Art. 61, Ley 28237, 31 de mayo de 2004, Código Procesal Constitucional. Y tal como consta analizado respecto de los titulares del derecho fundamental a la protección de datos personales, son titulares activos de la acción de *habeas data* tanto la persona natural como la jurídica.	**Titulares, encargados y terceros.** Según el artículo 61 del citado Código Procesal Constitucional, serán sujetos pasivos de la acción constitucional de *habeas data*, las entidades, públicas o de instituciones privadas que traten, generen, produzcan, procesen o posean, o aquellas instituciones privadas que brinden servicio o acceso a terceros. Y según el artículo 28 de la Ley de Protección de Datos los titulares, encargados y terceros	**Solicitar información y a la protección de datos personales.** El artículo 61 del Código Procesal Constitucional señala expresamente que los derechos protegidos por el *habeas data* constan reconocidos en los incisos 5) y 6) del artículo 2 de la Constitución. En consecuencia, toda persona puede acudir a dicho proceso para proteger o tutelar el derecho a solicitar información pública y el derecho a la protección de datos personales.	El artículo 2 de la Ley 28237, 31 de mayo de 2004, Código Procesal Constitucional, señala que la procedencia de los procesos constitucionales de *habeas corpus*, amparo y *habeas data* opera cuando se amenace o viole los derechos constitucionales por acción u omisión de actos de cumplimiento obligatorio, por parte de cualquier autoridad, funcionario o persona. Cuando se invoque la amenaza de violación, esta debe ser cierta y de inminente realización. El proceso de cumplimiento procede para que se acate una norma legal o se ejecute un acto administrativo.	**Agotada la vía administrativa.** El artículo 24 de la Ley de Protección de Datos del Perú señala que el titular o el encargado del banco de datos personales que deniegue al titular de datos personales, total o parcialmente, el ejercicio de los derechos establecidos en esta ley, puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de *habeas data*.
República Dominicana	El artículo 70 de la Constitución de República Dominicana reconoce, por primer vez, la acción judicial de *habeas data*, por la cual toda persona tiene derecho "a conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística".	NO.	NO.	**Toda persona.** Las normas constitucionales citadas establecen que al sujeto activo como toda persona. El artículo 18 de la Ley 172-13 establece que la acción de protección de los datos personales o de *habeas data* será ejercida por el afectado, sus tutores, los sucesores o sus apoderados. Cuando la acción judicial sea ejercida por personas jurídicas deberá ser interpuesta por sus representantes legales o los apoderados que estas designen a tal efecto.	**Responsables y usuarios.** El artículo 19 de la Ley 172-13 dispone que la acción judicial procederá con respecto a los responsables y usuarios de bancos de datos públicos y privados destinados a proveer informes, cuando actúen contrario a las disposiciones establecidas en la presente ley.	**Intimidad y el honor personal, al respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo, así como al derecho al honor, al buen nombre y a la propia imagen y la protección de datos personales.** Art. 17, Ley 172-13. Los derechos tutelados por el *habeas data* son los de acceso, rectificación, supresión, cancelación o actualización.	El artículo 17 de la Ley 172-13 dispone que, sin perjuicio de los mecanismos establecidos para el ejercicio de los derechos de los interesados, estos podrán ejercer la acción judicial de *habeas data* para tomar conocimiento de la existencia de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados que se deriven de una relación comercial, laboral o contractual con una entidad pública o privada; o simplemente, para tomar conocimiento de los datos personales que se presuma que existen almacenados en archivos, registros o bancos de datos públicos o privados.	El artículo 20 señala que será competente para conocer de esta acción, el juez del domicilio del demandado, y para el caso de pluralidad de demandados, en el domicilio de uno de ellos. Y el procedimiento aplicable consta descrito en el artículo, que menciona que la acción de *habeas data* se tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo. El registro o el banco de datos, mientras dure el procedimiento, debe asentar o publicar en los informes que la información cuestionada está sometida a un proceso judicial o de impugnación de *habeas data*.
Uruguay	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.

Fuente y elaboración: La autora (2018).

1.5.8 Institucionalidad de protección

Respecto del derecho a la intimidad y a la privacidad, desde esta perspectiva, se colige lo siguiente:

Tabla 55

País	Ente rector	Contenido en el principio de calidad	Contenido en otros principios
El Salvador	Instituto de Acceso a la Información Pública (ámbito público)	Con la aclaración de que la Ley 534-2011 tiene como ámbito de aplicación el público, la institución que elabora los formularios para solicitudes de acceso a la información, solicitudes referentes a datos personales y solicitudes para interponer el recurso de apelación (art. 58); establecer los lineamientos para el manejo, mantenimiento, seguridad y protección de los datos personales y de la información pública, confidencial y reservada en posesión de las dependencias y entidades, y por tanto protege los datos personales en el sector público es el Instituto de Acceso a la Información Pública; el cual estará integrado por cinco comisionados y sus respectivos suplentes, quienes serán nombrados por el Presidente de la República (art. 52, Ley 534-2011).	
Venezuela	NO.	NO.	
Bolivia	NO.	NO.	
Chile	NO.	NO.	
Honduras	NO.		
Paraguay	NO.	NO.	

Fuente y elaboración: La autora (2018).

De lo analizado en la tabla 55, solo El Salvador tiene una institución que regula los datos personales con una visión acotada al ámbito público en el primer caso, el resto de países lamentablemente carecen de institucionalidad de protección.

a) Respecto del derecho a la protección de datos personales:

Tabla 56

País	Nombre de la autoridad reguladora	Norma
Argentina	Dirección Nacional de Protección de Datos Personales	Esta Dirección tendrá las funciones de asistir y asesorar a las personas para la defensa de los derechos de autodeterminación informativa y protección de datos personales; dictar las normas y reglamentaciones que desarrollen estos derechos; realizar un censo de archivos, registros o bancos de datos y mantener el registro permanente de los mismos; controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos; solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la ley. También, solicitar información a las entidades públicas; imponer sanciones administrativas de ser el caso y controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes.
Brasil	Autoridad Nacional Brasileña de Protección de Datos, ANPD	Art. 55-A. La Autoridad Nacional de Protección de Datos (ANPD), un organismo de administración pública federal que es miembro de la Presidencia de la República, se crea sin aumentar los gastos. Párrafo 1. La naturaleza legal de la ANPD es transitoria y puede ser transformada por el Poder Ejecutivo en una entidad de administración pública federal indirecta, sujeta a un régimen municipal especial y vinculada a la Presidencia de la República. (Incluido por la Ley N ° 13.853 de 2019) Párrafo 2. La evaluación con respecto a la transformación prevista en el Párrafo 1 de este artículo se llevará a cabo dentro de los dos (2) años a partir de la fecha de entrada en vigor de la estructura de régimen de la ANPD. Se le otorga naturaleza transitoria, pues al cabo de dos años, deberá ser evaluada y a discreción del gobierno, podrá transformarse en una autarquía vinculada a la Presidencia de la República.

Colombia	Superintendencia de Industria y Comercio (SIC)	"La Ley 1581 de Protección de Datos Personales de 2012 otorga a la Superintendencia de Industria y Comercio (SIC), la competencia de vigilar el tratamiento de datos personales y garantizar que se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley. Además, con esta Ley se introdujo el Registro nacional de bases de datos, administrado por la SIC para la debida inscripción de las mismas, siempre y cuando contengan datos personales. Asimismo, se faculta a la SIC para imponer sanciones pecuniarias a los responsables del tratamiento de datos que no cumplan las políticas de protección establecidas en la ley, las cuales consisten en multas, suspensión de actividades y suspensión definitiva de las operaciones en caso de que involucren tratamiento de datos".
Costa Rica	La Agencia de protección de Datos de los Habitantes	Ente adscrito al Ministerio de Justicia y Paz, que entró en funcionamiento el 5 de marzo del 2013 a partir de la vigencia del Reglamento a la Ley 8968.
Ecuador	NO.	NO.
Guatemala	Procurador de los Derechos Humanos	Art. 46, Decreto 57-2008, 23/09/2008. Autoridad reguladora. El acceso a la información pública como derecho humano fundamental previsto en la Constitución Política de la República de Guatemala y los tratados o convenios internacionales en esta materia, ratificados por el Estado de Guatemala, estará protegido por el Procurador de los Derechos Humanos en los términos de la Ley de la Comisión de los Derechos Humanos del Congreso de la República y del Procurador de los Derechos Humanos. Decreto 54-86 del Congreso de la República.
México	El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)	INAI es el organismo cuya finalidad es la de dirigir y coordinar el Sistema Nacional de Transparencia, por intermedio de su Presidente, quien además lo es también del Consejo Nacional del Sistema.
Nicaragua	Dirección de Protección de Datos Personales	La entidad encargada de velar por el cumplimiento y efectiva vigencia del derecho a la protección de datos personales es la Dirección de Protección de Datos Personales, conforme consta en el artículo 28. Cuyas funciones constan descritas en el artículo 29, incluyendo la obligación de habilitar el registro de ficheros de datos. Art. 28, Creación de la Dirección de Protección de Datos Personales. Créase la Dirección de Protección de Datos Personales, adscrita al Ministerio de Hacienda y Crédito Público, que contará con un Director designado por la máxima autoridad administrativa de dicho ministerio, y que tiene por objeto el control, supervisión y protección del tratamiento de los datos personales contenidos e ficheros de datos de naturaleza pública y privada.
Panamá	Autoridad Nacional de Transparencia y Acceso a la Información a través de su Dirección.	Artículo 36 LGPD. La Autoridad Nacional de Transparencia y Acceso a la Información, a través de la Dirección creada para conocer esta materia, está facultada para sancionar a la persona natural o jurídica responsable del tratamiento de los datos personales, así como al custodio de la base de datos, que por razón de la investigación de las quejas o denuncias que se les presenten y se les compruebe que han infringido los derechos del titular de los datos personales.
Perú	Autoridad Nacional de Protección de Datos Personales, dependiente de la Dirección Nacional de Justicia del Ministerio de Justicia	La Ley de Protección de Datos Personales, en el artículo 32, señala como órgano competente para proteger este derecho fundamental a la Autoridad Nacional de Protección de Datos Personales, dependiente de la Dirección Nacional de Justicia del Ministerio de Justicia. Goza de potestad sancionadora, así como de potestad coactiva. La Autoridad Nacional de Protección de Datos Personales debe presentar periódicamente un informe sobre sus actividades al Ministro de Justicia.
República Dominicana	Superintendencia de Bancos, respecto únicamente de datos crediticios	El artículo 29 de la Ley 172-13 señala que los archivos, registros o bancos de datos, públicos o privados, destinados a proveer informes crediticios estarán sujetos a la inspección y vigilancia de la Superintendencia de Bancos como órgano de control, incluso antes del inicio de actividades. Las Sociedades de Información Crediticia (SIC) deberán inscribirse en el registro público de Sociedad de Información Crediticia (SIC) que estará a cargo de dicha Superintendencia (art. 34). No consta otra autoridad de protección para las otras finalidades de los datos personales.
Uruguay	Unidad Reguladora y de Control de Datos Personales	La Ley 18.331 crea como órgano de control desconcentrado a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic) en la cual existe la Unidad Reguladora y de Control de Datos Personales, que está dotada de la más amplia autonomía técnica (art. 31).

Fuente y elaboración: La autora (2018).

De lo analizado en la tabla 56, se concluye que varios países tienen instituciones autónomas e independientes cuya competencia exclusiva es la protección de datos personales, tales como: Argentina, mediante la Dirección Nacional de Protección de

Datos Personales; Brasil, a través de la Autoridad Nacional Brasileña de Protección de Datos, ANPD; Costa Rica y la Agencia de protección de Datos de los Habitantes; Nicaragua, mediante la Dirección de Protección de Datos Personales, adscrita al Ministerio de Hacienda y Crédito Público.

México es un caso especial, pues el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) se dedica, tanto a la protección del dato público como del dato personal. Un caso que emula el modelo mexicano es el aprobado por Panamá que establece a la Autoridad Nacional de Transparencia y Acceso a la Información, a través de una de sus Direcciones, la competencia de control de protección de datos personales y para lo cual además, crea el Consejo de Protección de Datos Personales como ente consultivo en la materia de protección de datos personales, artículo 34 de la Ley 81. Uruguay, por intermedio de la Unidad Reguladora y de Control de Datos Personales, que es parte de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic).

Existen países que atribuyen la competencia de proteger los datos personales a instituciones que tienen otras competencias como el caso de: Colombia, por medio de la Superintendencia de Industria y Comercio (SIC); Perú, mediante la Autoridad Nacional de Protección de Datos Personales, dependiente de la Dirección Nacional de Justicia del Ministerio de Justicia

De otro lado, Guatemala protege de forma limitada solo las bases públicas por intermedio del Procurador de los Derechos Humanos

República Dominicana, por medio de la Superintendencia de Bancos respecto únicamente de datos crediticios.

Finalmente, Ecuador y Panamá no cuentan ni con instituciones ni competencias atribuidas a las existentes.

1.5.9 Régimen sancionador

Respecto del derecho a la intimidad y a la privacidad, desde esta perspectiva, se colige lo siguiente:

Tabla 57

País	Responsabilidad civil, penal y administrativa	Infracciones y sanciones
El Salvador	**Responsabilidad administrativa.** Imputación de responsabilidad de servidor público: Si el Comisionado designado encontrare los elementos necesarios para atribuir a un servidor público la presunta comisión de una infracción, dentro de los tres días hábiles posteriores a su designación, lo remitirá al pleno del Instituto para que resuelva sobre la imputación dentro de un plazo no mayor de tres días hábiles. El servidor público dispondrá de siete días hábiles contados a partir de la notificación para rendir su defensa, conforme el artículo 89. Cuando el Instituto determine durante la sustanciación del procedimiento que algún servidor público pudo haber incurrido en responsabilidad penal, deberá hacerlo del conocimiento del titular de la dependencia o entidad responsable y de la Fiscalía General de la República, en su caso, para que inicien el procedimiento de responsabilidad que corresponda. Asimismo, dará inicio el incidente	Naturaleza de las infracciones: De conformidad con los artículos 76, 77, 78 y 79, las infracciones muy graves se refieren a la sustracción, destrucción, ocultamiento o cualquier tipo de daño o manejo inadecuado de la información que se encuentre bajo custodia o difusión de aquella con carácter de reservada o confidencial o por la no entrega de información previamente ordenada por el Instituto. Las infracciones graves son aquellas relativas a un actuar negligente respecto de la contestación a las solicitudes de acceso a la información o en la difusión de la información a que están obligados conforme a esta ley o manejo inadecuado de información reservada. Las infracciones leves se refieren a obstáculos para la entrega de información en su tiempo y debida forma.

	sancionatorio ante el mismo Instituto (art. 100). Impugnación por particulares en proceso contencioso administrativo: También podrá iniciarse el procedimiento de aplicación de sanciones mediante denuncia escrita de cualquier persona, en la cual se expondrá en detalle los hechos constitutivos de cualquiera de las sanciones e infracciones previstas en la presente ley y anexará las pruebas que tuviera en su poder, conforme el artículo 76.	
Venezuela	NO.	NO.
Bolivia	**Responsabilidad penal.** En caso de incumplimiento de la acción de protección a la privacidad, por orden de la autoridad que conoció de la acción se remitirá al Ministerio Público para su procesamiento penal por atentado contra las garantías constitucionales (art. 131).	NO.
Chile	El artículo 23 de la Ley 19628 señala que la acción de *habeas data* podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción.	NO.
Honduras	NO.	NO.
Paraguay	**Responsabilidad administrativa.** Este régimen sancionador es de carácter administrativo. En la Ley 1682-2001 constan descritas, en el artículo 10, las sanciones que deberán aplicarse a varios supuestos de transgresión.	Se aplican cuando las personas físicas o jurídicas transgredan las obligaciones que constan descritas en la ley como publicar o distribuir información sobre situación patrimonial, solvencia económica o cumplimiento de obligaciones comerciales, negativa a rectificar o a suministrar información o lo hagan fuera de los plazos establecidos. Las sanciones serán multas económicas que podrán aumentar en caso de reincidencia. Además de la multa, el juzgado ordenará que se efectúen las rectificaciones o supresiones que correspondan, y podrá ordenar también que la sentencia definitiva sea publicada en forma total, parcial o resumida, a costa del responsable. Será competente para la aplicación de las multas el Juzgado en lo Civil y Comercial, en trámite sumario.

Fuente y elaboración: La autora (2018).

De lo analizado en la tabla 57, solo El Salvador establece responsabilidad civil, penal y administrativa, mientras que Paraguay solo menciona la responsabilidad administrativa, Bolivia responsabilidad penal y el caso de Chile que permite la reclamación mediante el *habeas data*. Asimismo, solo El Salvador y Paraguay determinan expresamente infracciones con sus respectivas sanciones.

a) Respecto del derecho a la protección de datos personales:

Tabla 58

País	Régimen sancionador	Descritas infracciones y sanciones
Argentina	**Responsabilidades civiles, administrativas y penales.** El artículo 31 LPDP, contenido en el Capítulo VI sobre Sanciones Administrativas, señala que los responsables de ficheros o lo usuarios en el caso del cometimiento de infracciones serán responsables administrativa, civil y penalmente, con sanciones de apercibimiento, suspensión o multas.	El Decreto 1558, Reglamento LPDP, contiene la descripción de las acciones consideradas infracciones, las sanciones, los procedimientos para la aplicación de estas sanciones, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.
Brasil		
	Art. 52 LGPD. Los agentes de procesamiento de datos, debido a violaciones de las normas previstas en esta Ley, están sujetos a las siguientes sanciones administrativas aplicables por la	Art. 53.LGPD La autoridad nacional definirá, mediante su propio reglamento sobre sanciones administrativas por infracciones de esta Ley, que estará sujeto a consulta pública, las metodologías que guiarán el cálculo del valor base de las multas.

	autoridad nacional: (…) Párrafo 2. Las disposiciones de este artículo no reemplazan la aplicación de sanciones administrativas, civiles o penales definidas en la Ley N ° 8.078, del 11 de septiembre de 1990, y en la legislación específica.	
Colombia	**Responsabilidades civiles, administrativas y penales.** La jurisprudencia colombiana señala la necesidad de una institucionalidad administrativa aun existiendo un régimen de control judicial, esto debido a que no es suficiente una protección reactiva ante la existencia de un daño inminente o real sino principalmente una preventiva que evite la transgresión y permita una tutela efectiva del derecho.	El artículo 23 señala las sanciones que la Superintendencia de Industria y Comercio podrá imponer a los responsables y encargados del tratamiento, que incluyen multas, suspensión de las actividades relacionadas con el tratamiento, actos correctivos; cierre temporal, inmediato y definitivo de las operaciones relacionadas con el tratamiento incluidos los datos sensibles. Las sanciones indicadas en el presente artículo solo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva. Finalmente, el artículo 24 señala los criterios para graduar las sanciones antes descritas, entre los cuales están la dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley; el beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción; la reincidencia en la comisión de la infracción; la resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio; la renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio; y, el reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar. Normas que establecen mecanismo o políticas internas efectivas que permitan demostrar la responsabilidad constan en los artículo 26 y 27 del Decreto número 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Costa Rica	**Responsabilidad administrativa**	Faltas, sanciones y procedimiento. La descripción de las sanciones se encuentra en el artículo 28 de la Ley 8968 que las clasifica en faltas leves, graves y gravísimas. Las primeras, faltas leves, atinentes a la recolección, almacenaje, y transmisión de datos personales para su uso en base de datos sin que se le otorgue suficiente y amplia información a la persona interesada o no se garanticen la seguridad e inalterabilidad de los datos.
Ecuador	NO.	NO.
Guatemala	NO.	NO.
México	**Responsabilidades civiles, administrativas y penales**	Tanto la LFPDPPP de 2010 como la LGPDPPSO de 2017 señalan expresamente un procedimiento de Imposición de Sanciones, que con motivo del procedimiento de protección de derechos o del procedimiento de verificación que realice el Instituto, cuando existiere indicios de un presunto incumplimiento se iniciará este procedimiento, a efecto de determinar la sanción que corresponda (artículo 61). Pero esta última añade las medidas de apremio para lograr el cumplimiento conminatorio de las resoluciones dictadas.
Nicaragua	**Responsabilidades civiles, administrativas y penales**	Respecto de la administrativa se encuentran descritos los tipos de infracción que van desde las leves hasta las graves en el artículo 45. Así como en el artículo 46 se determinan las sanciones administrativas de los responsables o usuarios de los ficheros de datos.
Panamá	**Responsabilidad administrativas en el ejercicio de la garantía de *habeas data***	Conforme el artículo 20 de la Ley 6 de 2002, sobre *habeas data* el capítulo VI, relativo las Sanciones y Responsabilidades Personales de los Funcionarios que sus artículos pertinentes determina: Artículo 20. El funcionario requerido por el Tribunal que conoce del recurso de *habeas data*, que incumpla con la obligación de suministrar la información incurrirá en desacato y será sancionado con multa mínima equivalente al doble del salario mensual que devenga. En caso de reincidencia, el funcionario será sancionado con la destitución del cargo. El Art. 38.señala que "Las infracciones a esta Ley se clasifican en leves, graves o muy graves". .En el Art. 39 se describen las infracciones leves; el Art. 40; las infracciones graves; el Art. 41 las infracciones muy graves.
Perú	**Responsabilidades civiles, administrativas y penales**	"El Título VII sobre Infracciones y Sanciones Administrativas de la Ley de Protección de Datos Personales señala en los artículos 37 a 40. El Procedimiento sancionador, infracciones leves, graves y muy graves, sanciones administrativas y multas coercitivas, respectivamente. Respecto al procedimiento sancionador, este se inicia de oficio, por parte de la Autoridad Nacional de Protección de Datos Personales o por denuncia de parte, ante la presunta comisión de actos contrarios a lo dispuesto en la presente Ley o en su reglamento. Las resoluciones de la Autoridad Nacional de Protección de Datos Personales agotan la vía administrativa. Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa. Respecto de la calificación, la graduación del monto de las multas, el procedimiento para su aplicación y otras tipificaciones constan descritos en el reglamento a la Ley. Respecto de sanciones civiles consta lo dispuesto en el artículo 39 de la citada Ley que señala que la imposición de la multa se efectúa sin perjuicio de las sanciones disciplinarias sobre el personal de las entidades públicas en los casos de bancos de datos personales de administración pública, así como de la indemnización por daños y perjuicios y de las sanciones penales a que hubiera lugar".
República Dominicana	**Responsabilidades civiles, administrativas y penales**	Se establecen varios regímenes aplicables a distintos ámbitos: *Sanciones administrativas para las Sociedades de Información Crediticia*: El artículo 81 establece las sanciones administrativas propias de las Sociedades de Información Crediticia (SIC) que serán establecidas por la Superintendencia de Bancos. En caso de fallo adverso a la Sociedad de Información Crediticia (SIC) ante el Tribunal Superior Administrativo, la Sociedad de Información Crediticia (SIC) dispone de un plazo de un (1) mes para recurrir en casación, de conformidad con la ley que instituye el Procedimiento de Casación. La Superintendencia de Bancos no puede ejercer las facultades estipuladas en la presente ley en perjuicio de una Sociedad de Información Crediticia (SIC) hasta tanto no intervenga

		una decisión definitiva y con la autoridad de la cosa irrevocablemente juzgada (art. 83). *Sanciones excepcionales:* El artículo 84 señala que será sancionado con una multa de diez (10) a cincuenta (50) salarios mínimos vigentes, sin perjuicio de las reparaciones que procedan por los daños y perjuicios que haya sufrido la persona por causa de violación a su derecho a la privacidad, conforme a las normas del derecho común, la persona física que: 1. Insertara o hiciera insertar, a sabiendas, datos falsos en un archivo de datos personales, de manera dolosa o de mala fe. 2. Proporcionará, de manera dolosa o de mala fe, información falsa a un tercero, contenida en un archivo de datos personales. 3. Accediere a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, de cualquier forma, a un banco de datos personales. 4. Revelare a otra información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley. *Sanciones civiles:* el artículo 85 dispone que agotado el procedimiento de solicitud y rectificación establecido en la presente ley, se considerarán infracciones civiles: 1. Denegar, sin fundamento, una solicitud de revisión o una solicitud de rectificación de la información crediticia requerida por el titular de la información. 2. Negarse a modificar o a cancelar la información de un titular de la información, luego de que éste haya obtenido un pronunciamiento favorable en un procedimiento seguido de conformidad con lo establecido en la presente ley. 3. Infringir de manera grave o reiterada las disposiciones de las sentencias de los tribunales civiles con la autoridad de la cosa irrevocablemente juzgada. *Sanciones penales:* el artículo 86 señala que en caso de que un usuario o suscriptor haya accedido a una base de datos para consultar, de manera fraudulenta, las informaciones personales de un titular sin haber obtenido de éste autorización previa, será sancionado con multa que irá de diez (10) a cincuenta (50) salarios mínimos vigentes, sin perjuicio de las reparaciones que procedan por los daños y perjuicios que haya sufrido la persona por causa de violación a su derecho a la privacidad, conforme a las normas del derecho común. Al usuario o suscriptor o cualquier persona física que utilice o facilite un reporte de crédito, con la finalidad de la comisión de un delito, se impondrá una sanción equivalente a prisión correccional de seis meses a dos años. Se considerará una circunstancia agravante del crimen imputado el hecho de que un usuario o suscriptor haga uso de un reporte de crédito, con la finalidad de la comisión de un crimen
Uruguay	**Responsabilidades civiles, administrativas y penales**	La Unidad Reguladora y de Control de Datos Personales, tendrá potestades sancionatorias, por las cuales el órgano de control podrá aplicar las siguientes medidas sancionatorias a los responsables de las bases de datos o encargados del tratamiento de datos personales en caso de que se violen las normas de la presente ley: a) apercibimiento; b) multa de hasta quinientas mil unidades indexadas; c) suspensión de la base de datos respectiva. A tal efecto se faculta a la AGESIC a promover ante los órganos jurisdiccionales competentes, la suspensión de las bases de datos, hasta por un lapso de seis días hábiles, respecto de los cuales se comprobare que infringieren o transgredieren la presente ley

Fuente y elaboración: La autora (2018).

De acuerdo con lo analizado en la tabla 58, excepto Ecuador y Guatemala en los que no existe responsabilidad administrativa sino únicamente civil y penal, todos los otros países analizados tienen los tres tipos de responsabilidad. Excepto esos mismos países, y Brasil que desarrollará en reglamento la lista de infracciones, todos los otros países establecen infracciones debidamente tipificadas con sus respectivas sanciones por el incumplimiento de las obligaciones relativas a la protección de los datos personales, estas conductas transgresoras en su mayoría se sancionan con multas de contenido económico.

1.5.10 Transferencia internacional de datos:

Respecto del derecho a la intimidad y a la privacidad, desde esta perspectiva, se colige lo siguiente:

Tabla 59

País	**Transferencia internacional de datos**
El Salvador	NO.
Venezuela	NO.
Bolivia	NO.
Chile	NO.
Honduras	NO.
Paraguay	NO.

Fuente y elaboración: La autora (2018).

De lo analizado en la tabla 59, ninguno de los países analizados contempla normativa sobre transferencia internacional de datos, lo que demuestra la necesidad de una normativa específica enfocada a la protección de datos personales y no solo la intimidad y la privacidad.

a) Respecto del derecho a la protección de datos personales:

Tabla 60

País	Descripción del concepto de transferencia internacional de datos	Referencia a nivel adecuado de protección	Declaración de país con nivel adecuado	Avisos de privacidad	Entre responsable y encargado
Argentina	NO.	El artículo 12 de la LPDP señala que respecto de la transferencia internacional está prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.	NO.	NO.	NO.
Brasil	NO.	SI. El Art. 33 LGPD determina que la transferencia internacional de datos personales solo está permitida en los siguientes casos: países con niveles adecuados, garantías de cumplimiento, cooperación jurídica internacional, ejecución de competencias públicas, consentimiento del titular específico,	NO.	NO	NO
Colombia	NO.	Según el artículo 26 de la Ley 1581: "Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos".	Según el artículo 26 de la Ley 1581: "Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios".	NO.	NO.
Costa Rica	**NO menciona datos transfronterizos** Consta en el artículo 14 norma expresa que regula la transferencia de datos personales, públicas o privadas, que solo podrán transferir datos contenidos en ellas "cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar" los principios y derechos reconocidos en esta ley.	NO.	NO.	NO.	NO.
Ecuador	NO.	NO.	NO.		
Guatemala	NO.	NO.	NO.		
México	Art. 66. Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes. Lo dispuesto en el párrafo anterior, no será aplicable en los siguientes casos: I. Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a estos. II. Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o	Art. 68. El responsable solo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obligue a proteger los datos personales conforme a los principios y deberes que establece la presente ley y las disposiciones que resulten aplicables en la materia.	NO.	En la LFPDPPP de 2010 consta el capítulo V titulado "De la Transferencia de Datos", por el cual el responsable que pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a estos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus	Art. 71. Las remisiones nacionales e internacionales de datos personales que se realicen entre responsable y encargado no requerirán ser informadas al titular, ni contar con su consentimiento.

	bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquellas que dieron origen al tratamiento del responsable transferente.			datos; de igual manera, el tercero receptor asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos (art. 36).	
Nicaragua	NO.	Art. 14, Ley 787. Prohibiciones y excepciones de cesión y transferencia de datos. Se prohíbe la cesión y transferencia de datos personales de cualquier tipo con países u organismos internacionales, que no proporcionen niveles de seguridad y protección adecuados.	NO.	NO.	NO.
Panamá	SI. Art. 4 numeral 19 se entiende por transferencia de datos el: (…) dar a conocer, divulgar, comunicar, intercambiar y/o transmitir, de cualquier forma y por cualquier medio, de un punto a otro, intra o extrafronterizo, los datos a personas naturales o jurídicas distintas del titular, ya sean determinadas o indeterminadas.	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes: 2. Que le país u organismo internacional o supranacional receptor proporcione un nivel de protección equivalente o superior.	NO.	NO.	NO.
Perú	El artículo 2 de la ley de la materia señala entre las definiciones el de flujo transfronterizo de datos personales, aquella transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.	Finalmente, el artículo 15 determina que el titular y el encargado del banco de datos personales deben realizar el flujo transfronterizo de datos personales solo si el país destinatario mantiene niveles de protección adecuados conforme a la presente ley.	Según el numeral 10, el nivel suficiente de protección para los datos personales abarca por lo menos la consignación y el respeto de los principios rectores de la ley citada, así como medidas técnicas de seguridad y confidencialidad.	NO.	NO.
República Dominicana	NO.	La transferencia internacional de datos personales de cualquier tipo con países u organismos internacionales o supranacionales.	NO.	NO.	
Uruguay	El Decreto 414/009 determina en el artículo 4, relativo a las definiciones aplicables a la materia, el concepto de transferencia internacional de datos, por el cual constituye el tratamiento de datos que supone una transmisión de estos fuera del territorio nacional, constituyendo una cesión o comunicación, y teniendo por objeto la realización de un tratamiento por cuenta del responsable de la base de datos o tratamiento establecido en territorio uruguayo.	El artículo 23 de la Ley 18.331 "prohíbe la transferencia de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia".	Art. 23, Ley 18.3331. Sin perjuicio de lo dispuesto en el primer inciso de este artículo, la Unidad Reguladora y de Control de Protección de Datos Personales podrá autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes respecto a la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos. Dichas garantías podrán derivarse de cláusulas contractuales apropiadas.	NO.	Art. 23, Ley 18.3331. "C) Que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero".

Fuente y elaboración: La autora (2018).

Tabla 61

País	Autorización o consentimiento	Relación jurídica u obligación legal o reglamentaria	Contratos	Interés público o entre responsables públicos	Pruebas o garantías de cumplimiento de los principios, los derechos y el régimen de protección de datos (cláusulas contractuales, códigos tipo, etc.)	Judicial	Colaboración judicial internacional	Salud	Transferencias bancarias y bursátiles	Sociedades	Tratados internacionales	Lucha contra el crimen organizado, terrorismo y narcotráfico
Argentina	NO.	NO.	NO.	NO.	NO.	NO.	Art. 12. "2. La prohibición no regirá en los siguientes supuestos: a) Colaboración judicial internacional".	Art. 12. "2. La prohibición no regirá en los siguientes supuestos: [...] b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los	Art. 12. "2. La prohibición no regirá en los siguientes supuestos: [...] c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable".	NO.	Art. 12. "2. La prohibición no regirá en los siguientes supuestos: [...] d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte".	Art. 12. "2. La prohibición no regirá en los siguientes supuestos: [...] e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico".

							términos del inciso e) del artículo anterior".				
Brasil	SI. Art. 33 LGPD.- La transferencia internacional de datos personales solo está permitida en los siguientes casos: (...) V - cuando la autoridad nacional autoriza la transferencia; VIII - cuando el titular haya dado su consentimiento específico y destacado a la transferencia, con información previa sobre el carácter internacional de la operación, distinguiéndola claramente de otros fines; o	SI. Art. 33 LGPD.- La transferencia internacional de datos personales solo está permitida en los siguientes casos: (...) IX - cuando sea necesario para cumplir con las hipótesis previstas en los artículos II, V y VI del art. 7 de esta Ley. El numeral II del artículo 7 señala: "(...) II - para el cumplimiento de la obligación legal o reglamentaria por parte del controlador;(...)"	SI. Art. 33 LGPD.- La transferencia internacional de datos personales solo está permitida en los siguientes casos: (...) IX - cuando sea necesario para cumplir con las hipótesis previstas en los artículos II, V y VI del art. 7 de esta Ley. El numeral V del artículo 7 señala: "(...) V - cuando sea necesario para la ejecución del contrato o procedimientos preliminares relacionados con el contrato del cual el titular es parte, a solicitud del interesado;	SI. Art. 33 LGPD.- La transferencia internacional de datos personales solo está permitida en los siguientes casos: (...) VII - cuando la transferencia sea necesaria para la política pública de ejecución o autoridad legal de servicio público, que se hizo público, de conformidad con la sección I de la cápita de arte. 23 de esta Ley; Párrafo único. A los efectos del punto I de este artículo, las personas jurídicas de derecho público a que se refiere el único párrafo del art. 1 de la Ley N ° 12.527, de 18 de noviembre de 2011 (Ley de Acceso a la Información), dentro del alcance de sus competencias legales, y el responsable, dentro del alcance de sus actividades, puede solicitar a la autoridad nacional que evalúe el nivel de protección de los datos personales. conferido por país u organismo internacional.	SI. SI. Art. 33 LGPD.- La transferencia internacional de datos personales solo está permitida en los siguientes casos: (...) II - cuando el controlador ofrece y prueba garantías de cumplimiento de los principios, los derechos del titular y el régimen de protección de datos previsto en esta Ley, en forma de: a) cláusulas contractuales específicas para una transferencia dada; b) cláusulas contractuales estándar; c) estándares corporativos globales; d) sellos, certificados y códigos de conducta emitidos regularmente;	SI. Art. 33 LGPD.- La transferencia internacional de datos personales solo está permitida en los siguientes casos: (...) IX - cuando sea necesario para cumplir con las hipótesis previstas en los artículos II, V y VI del art. 7 de esta Ley. El numeral VI del artículo 7 señala: "(...) VI - para el ejercicio regular de derechos en procedimientos judiciales, administrativos o arbitrales, este último de conformidad con la Ley N ° 9.307, de 23 de septiembre de 1996 (Ley de Arbitraje) ;(...)"	SI. Art. 33 LGPD.- La transferencia internacional de datos personales solo está permitida en los siguientes casos: (...) VI - cuando la transferencia resulta en un compromiso hecho en un acuerdo de cooperación internacional;	SI. Art. 33 LGPD.- La transferencia internacional de datos personales solo está permitida en los siguientes casos: (...) IV - cuando la transferencia es necesaria para proteger la vida o la seguridad física del titular o de un tercero;	NO.	NO.	SI. Art. 33 LGPD.- La transferencia internacional de datos personales solo está permitida en los siguientes casos: (...) III - cuando la transferencia sea necesaria para la cooperación jurídica internacional entre los organismos de inteligencia pública, investigación y enjuiciamiento, de conformidad con los instrumentos del derecho internacional;
Colombia	Art. 26. "Esta prohibición no regirá cuando se trate de: a. Información respecto de la cual el Titular haya otorgado su	NO.	Art. 26. "(...) e. Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la	NO.	NO.	Art. 26. "f. Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento,	NO.	Art. 26. "b. Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por	Art. 26. "c. Transferencias bancarias o bursátiles, conforme a la legislación que les resulte	NO.	Art. 26. "d. Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el	NO.

	autorización expresa e inequívoca para la transferencia".		ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular".			ejercicio o defensa de un derecho en un proceso judicial".		razones de salud o higiene pública".	aplicable".		principio de reciprocidad".	
Costa Rica	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Ecuador	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
Guatemala	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.	NO.
México	Art. 37, LFPDPPP de 2010. Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos..." Art. 65, LGPDPSO. Toda transferencia de datos personales, sea esta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de esta ley. Art. 70, LGPDPSO. VIII. Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales,	Art. 37, LFPDPPP de 2010. VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular. Art. 70, LGPDPSO. "VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular".	Art. 37, LFPDPPP de 2010. IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero. Art. 70, LGPDPSO. "VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero".	Art. 37, LFPDPPP de 2010. V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia. Art. 70, LGPDPSO. "II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales".	NO.	Art. 37, LFPDPPP de 2010. "VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial". Art. 70, LGPDPSO. "III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia; IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última".	NO.	Art. 37, LFPDPPP de 2010. II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios. Art. 70, LGPDPSO. "V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos	NO	Art. 37, LFPDPPP de 2010. III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas".	Art. 37, LFPDPPP de 2010. I. Cuando la transferencia esté prevista en una ley o tratado en los que México sea parte. Art. 70. El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos: I. Cuando la transferencia esté prevista en esta ley u otras leyes, convenios o tratados internacionales suscritos y ratificados por México.	Art. 70, LGPDPSO. IX. Cuando la transferencia sea necesaria por razones de seguridad nacional.

	conforme a lo dispuesto en el artículo 22 de la presente Ley".							fines sean acreditados".				
Nicaragua	NO.	NO.	NO.	NO.	NO.	NO.	Art. 14, Ley 787. La prohibición no regirá en los supuestos de colaboración judicial internacional.	Art. 14, Ley 787. "intercambio de datos personales en materia de salud, cuando sea necesaria para una investigación epidemiológica".	Art. 14, Ley 787. "transferencias bancarias o bursátiles".	NO.	Art. 14, Ley 787. "conforme la legislación de la materia, cuando la transferencia se hubiere acordado en el marco de tratados internacionales ratificados por el Estado de Nicaragua".	Art. 14, Ley 787. "y cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia, en los delitos regulados en la Ley No. 735, "Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados", en los Delitos Relacionados con Estupefacientes, Psicotrópicos y otras Sustancias Controladas, Delitos Contra la Seguridad del Estado y Delitos Contra el Orden Internacional tipificados en la Ley No. 641", Código Penal, arts. 84, 85, 86 y 87.
Panamá	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes: 1. Que cuente con el consentimiento del titular de los datos.	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes: 9. Que sea necesaria para el mantenimiento o cumplimiento de una relación jurídica entre el responsable del tratamiento y el	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes: 6. Que sea necesaria en virtud de un contrato celebrado o por celebrar en interés inequívoco del titular de los datos, por el responsable del tratamiento y un	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes: 7. Que sea necesaria o legalmente exigida para la salvaguarda de un interés público o para la representación legal del titular de los datos personales o administración de	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes: 12. Que el responsable del tratamiento que transfiere los datos y el destinatario adopten mecanismos de autorregulación	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes: 8. Que sea necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, o en casos de colaboración	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes:	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes: (…) 4. Que sea necesaria para la prevención o el diagnóstico médico, la	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes: 10. Que sea requerida para concretar	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes: 5. Que se efectuada a cualquier	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes: (…) 3. Que se encuentre prevista en una ley o tratado en los que la Republica de Panamá sea parte. .	SI. Art. 33 Ley 81. Se entenderá que toda transferencia de datos personales es lícita si se cumple al menos una de las condiciones siguientes: (…) 11. Que tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, el lavado

		titular de los datos.	tercero.	justicia.	vinculante, siempre que estos sean acordes a las disposiciones previstas en esta Ley. 13. Que se realice en el marco de cláusulas contractuales que contengan mecanismos de protección de los datos personales acordes con las disposiciones previstas en la presente Ley, siempre que el titular sea parte.	judicial internacional.		prestación asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios.	transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable.	sociedad del mismo grupo económico del responsable del tratamiento, siempre que los datos personales no sean utilizados para finalidades distintas las que originaron su recolección.		de activos, los delitos informáticos, la pornografía infantil y el narcotráfico.
Perú	Art. 15, Ley 2793. "7. Cuando el titular de los datos personales haya dado su consentimiento previo, informado, expreso e inequívoco".	NO.	Art. 15, Ley 2793. "4. Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte, incluyendo lo necesario para actividades como la autenticación de usuario, mejora y soporte del servicio, monitoreo de la calidad del servicio, soporte para el mantenimiento y facturación de la cuenta y aquellas actividades que el manejo de la relación contractual requiera".	NO.	NO.	NO.	Art. 15, Ley 2793. "2. Cooperación judicial internacional".	Art. 15, Ley 2793. 6. "Cuando el flujo transfronterizo de datos personales se realice para la protección, prevención, diagnóstico otorgamiento médico o quirúrgico de su titular; o cuando sea necesario para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimiento de disociación adecuados".	Art. 15, Ley 2793. "5. Cuando se trate de transferencias bancarias o bursátiles, en lo relativo a las transacciones respetivas y conforme a la ley aplicable".	NO.	Art. 15, Ley 2793. Flujo transfronterizo de datos. "No se aplica lo dispuesto en el segundo párrafo en los siguientes casos: 1. Acuerdos en el marco de tratados internacionales sobre la materia en los cuales la República del Perú sea parte".	Art. 15, Ley 2793. "3. Cooperación internacional entre organismos de inteligencia para la lucha contra el terrorismo, tráfico ilícito de drogas, lavado de activos, corrupción, trata de personas y otras formas de criminalidad organizada".
República Dominica	El artículo 80 de la Ley 172-13 analizada señala	NO.	Art. 80, Ley 172-13 "6. La transferencia de datos sea necesaria	NO.	NO.	Art. 80, Ley 172-13. "7. La transferencia de	Art. 80, Ley 172-13. "9. La transferencia de datos se efectúe a	Art. 80, Ley 172-13. "2. Se trate de	Art. 80, Ley 172-13. "3. Se trate de	NO.	Art. 80, Ley 172-13. "4. La transferencia de datos se hubiera	Art. 80, Ley 172-13. "5. La transferencia de datos tenga por

na	que la transferencia internacional de datos personales de cualquier tipo con países u organismos internacionales o supra nacionales, que requieran del consentimiento del titular solo se efectuarán si: 1. La persona física, libre y conscientemente, decidiera autorizar por voluntad propia la transferencia de datos, o cuando las leyes lo permitan".		para la ejecución de un contrato entre el titular de los datos y el responsable del tratamiento, o para la ejecución de medidas precontractuales".			datos legalmente exigida sea para la salvaguarda del interés público o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, o solicitada por una administración fiscal o aduanera para el cumplimiento de sus competencias. 8. La transferencia de datos se efectúe para prestar o solicitar un auxilio judicial internacional".	petición de un organismo internacional con interés legítimo desde un registro público".	intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado o una investigación epidemiológica, o por razones de salud o higiene pública".	transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable".		acordado o contemplado en el marco de tratados internacionales o convenios, y en los tratados de libre comercio de los cuales sea parte la República Dominicana".	objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, la trata de personas, el narcotráfico, y demás crímenes y delitos".
Uruguay	Art. 23, Ley 18.3331. "También será posible realizar la transferencia internacional de datos en los siguientes supuestos: A) Que el interesado haya dado su consentimiento inequívocamente a la transferencia prevista".	NO.	Art. 23, Ley 18.3331. "B) Que la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado".	Art. 23, Ley 18.3331. "D) Que la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial". Art. 23, Ley 18.3331. "F) Que la transferencia tenga lugar desde un registro que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para su consulta".	NO.	NO.	Art. 23, Ley 18.331. "La prohibición no regirá cuando se trate de: Cooperación judicial internacional, de acuerdo al respectivo instrumento internacional, ya sea Tratado o Convención, atendidas las circunstancias del caso". E) Que la transferencia sea necesaria para la salvaguardia del interés vital del interesado".	Art. 23, Ley 18.3331. "2) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado por razones de salud o higiene públicas. [...]	Art. 23, Ley 18.3331. "3) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable".	NO.	Art. 23, Ley 18.3331. "4) Acuerdos en el marco de tratados internacionales en los cuales la República Oriental del Uruguay sea parte".	Art. 23, Ley 18.3331. "5) Cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico".

Fuente y elaboración: La autora (2018).

Sobre transferencias de datos personales cabe realizar los siguientes niveles de análisis:

- *Descripción del concepto de transferencia internacional de datos:* Únicamente, México, Panamá, Perú y Uruguay definen qué debe entenderse por transferencia internacional de datos. En el caso de México, además, determinan la necesidad de formalizar la transferencia mediante la suscripción de cualquier instrumento jurídico que cumpla la normativa y que avale el intercambio.
- *Referencia a nivel adecuado de protección:* Argentina, Brasil, Colombia, México, Panamá, Perú, República Dominicana y Uruguay establecen como condición necesaria que permite el intercambio internacional de datos que el país receptor proteja los datos conforme la normativa del país emisor (México) o que cumpla un estándar para que sea posible la transferencia. Que el país u organismo internacional o supranacional proporcione un nivel de protección equivalente o superior, como consta en la legislación panameña. Brasil establece como criterio de transferencia internacional y legal de datos personales que el país u organizaciones internacionales mantenga un grado de protección de datos personales adecuado.
- *Declaración de país con nivel adecuado:* La normativa colombiana establece una definición sobre nivel adecuado al señalar que consiste en un país que cumple con los estándares fijados por la Superintendencia de Industria y Comercio, y que en ningún caso serán inferiores a los que la conste en la ley. En el caso del Uruguay es la Unidad Reguladora y de Control de Protección de Datos Personales quien podrá autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes respecto a la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos. En estos casos, la declaración de nivel adecuado depende de la autoridad de control del país que va autorizar la transferencia internacional de datos, de tal manera que es su responsabilidad verificar si el otro país que va a recibir la data cumple con los estándares o niveles establecidos en su normativa en garantía de los derechos de sus ciudadanos. Por su parte Perú, señala que el nivel suficiente de protección para los datos personales abarca por lo menos la consignación y el respeto de los principios rectores de la ley citada, así como medidas técnicas de seguridad y confidencialidad. Es decir, los tres países en análisis basan la declaración de adecuado en los esquemas de protección establecidos por cada estado, pero en el caso de Perú, este hace hincapié en los elementos técnicos del tratamiento de datos para esta determinación de un nivel adecuado.
- *Avisos de privacidad:* México es el único país que establece la necesidad de que la transferencia de datos se realice implementando avisos de privacidad, por los cuales se solicita autorización y debe informar sobre las finalidades para las cuales se obtiene sus datos.
- *Entre responsable y encargado:* Únicamente México señala la excepción de que no se requerirán informar al titular, ni contar con su consentimiento para la cesión entre responsable y encargado.

Asimismo, se compara en la normativa de la región aquellos criterios coincidentes y disidentes respecto de la regla general de no transferir datos personales a menos que se trate de los aspectos siguientes:

- *Autorización por parte del titular:* La transferencia de datos personales, nacional o internacional, se encuentra sujeta al consentimiento de su titular conforme señala la normativa colombiana, de República Dominicana, México, Nicaragua, Perú y Uruguay.

- *Relación jurídica:* México y Nicaragua señalan otra excepción relativa al mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.
- *Contratos:* Colombia, República Dominicana, México, Nicaragua, Perú y Uruguay determinan como excepción la transferencia en virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero. Añadiéndose que en el caso de Perú se específica que esta autorización es para actividades como la autenticación de usuario, mejora y soporte del servicio, monitoreo de la calidad del servicio, soporte para el mantenimiento y facturación de la cuenta; mientras que Uruguay y República Dominicana determinan de forma genérica aquellas actividades propias del manejo de la relación contractual.
- *Interés público:* Colombia, México, Nicaragua Perú, República Dominicana y Uruguay señalan que la transferencia de datos sea necesaria o legalmente exigida para la salvaguarda de un interés público. Incluido el tema tributario como señala República Dominicana.
- *Entre responsables públicos:* México, Nicaragua y Uruguay determinan que la transferencia se realice entre responsables para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.
- *Asuntos judiciales:* Colombia, México, Nicaragua y República Dominicana señalan que la transferencia es posible cuando sea necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial o ante autoridad competente, así como la procuración o administración de justicia.
- *Colaboración judicial internacional:* Argentina, República Dominicana, Nicaragua, Perú y Uruguay reconocen esta excepción.
- *Salud:* Argentina, Colombia, República Dominicana, Nicaragua, Perú y Uruguay establecen que el intercambio de datos de carácter médico puede ser posible cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios. Perú, además, condiciona que los datos deben ser disociados.
- *Transferencias bancarias y bursátiles:* Es posible estas transferencias en lo relativo a las respectivas transacciones conforme consta en Argentina, Colombia, República dominicana, Nicaragua, Perú y Uruguay.
- *Sociedades:* Únicamente México establece esta excepción relativa a las transferencias efectuadas a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas.
- *Tratados internacionales:* Todas aquellas que estén previstas en leyes, convenios o tratados internacionales suscritos y ratificados, al tenor de lo señalado en Argentina, Colombia, Costa Rica, República Dominicana, México, Nicaragua, Perú y Uruguay.
- *Prevención, investigación y persecución del crimen organizado, terrorismo y narcotráfico, administración de los bienes incautados, decomisados y abandonados, delitos contra la seguridad del Estado, lavado de activos, corrupción, trata de personas y demás delitos:* Se autoriza el intercambio de datos cuando la transferencia sea legalmente exigida para la investigación y persecución de estos delitos, conforme señala Argentina, República Dominicana, México, Nicaragua, Perú y Uruguay.

Finalmente, Costa Rica, Ecuador, Guatemala, Panamá no señalan norma alguna relativa al flujo transfronterizo de datos.

1.5.11 Otros contenidos esenciales

A continuación, se enlistan varios contenidos esenciales que no constaban dentro de las configuraciones iniciales o que han podido identificarse como propios de las normativas latinoamericanas y que son parte de la normativa europea, y que en otros casos existe duda sobre su alcance. Sobre más detalle de su contenido consta descrito en el análisis de la legislación de cada país.

- *Principio de interés superior del niño, niña y adolescente:* Colombia establece la prohibición expresa de tratar datos personales de niños, niñas y adolescentes en virtud de este principio.
- *Procedimiento de anonimización:* Perú realiza expresa mención de la existencia de este tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos, anotándose que para que este se configure el procedimiento debe ser irreversible.
- *Procedimiento de disociación:* Perú determina expresamente que consiste en el tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos y que en este caso el procedimiento es reversible.
- *Código de Conducta:* Este es criterio que mayor coincidencia tiene en la legislación porque Argentina, Uruguay, México y República Dominicana lo reconocen en su normativa. Argentina determina que las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante, esquemas de mejores prácticas o códigos de conducta de práctica profesional, o códigos tipo que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la ley en la materia, que complementen lo dispuesto por la presente ley. Dichos esquemas deberán contener mecanismos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas eficaces en caso de incumplimiento. Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos y contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares. Finalmente, Costa Rica establece la posibilidad de que se incorporen protocolos de actuación, en los cuales se describan los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales. Para que sean válidos los protocolos de actuación, deberán ser inscritos, así como sus posteriores modificaciones, ante la Prodhab. La Prodhab podrá verificar, en cualquier momento, que la base de datos esté cumpliendo cabalmente con los términos de su protocolo.
- *Registro Nacional "No Llame":* Argentina tiene una iniciativa que consta en la Ley 26.951, de 5 de agosto de 2014, que determina la creación de un registro nacional denominado "No llame", cuya finalidad es la de proteger a toda persona física o jurídica, titular de servicios de telefonía, en cualquiera de sus modalidades, de los abusos del procedimiento de contacto, publicidad, oferta, venta y regalo de bienes o servicios no solicitados (art. 1). La inscripción y baja en el Registro es gratuita y deberá ser solicitada únicamente por el titular o usuario en cualquier momento y tendrá efectos inmediatos.
- *De las versiones públicas:* México determina que cuando un documento o expediente contenga partes o secciones reservadas o confidenciales, los sujetos obligados a efectos de atender una solicitud de información, deberán elaborar una versión pública en la que se transcriban las partes o secciones clasificadas, indicando su contenido de manera

genérica, fundando y motivando su clasificación. Si bien esta norma es aplicable a transparencia y acceso a la información pública, sin embargo, puede ser aplicable en aquellos casos en los que un documento contiene datos públicos y datos personales, por ejemplo, las sentencias judiciales.

- *Portabilidad de los datos:* México determina que cuando se traten datos personales por vía electrónica, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.
- *Prohibiciones a funcionarios de la Agencia:* Costa Rica señala que el personal técnico y administrativo de la Prodhab está obligado a guardar secreto profesional y deber de confidencialidad de los datos de carácter personal que conozca en el ejercicio de sus funciones.
- *Capacitación de los servidores públicos:* El Salvador establece que con la finalidad de promover una cultura de acceso a información en la administración pública, los entes obligados deben capacitar periódicamente a todos sus servidores públicos en materia del derecho de acceso a la información pública y el ejercicio del derecho a la protección de datos personales.
- *Promoción de cultura e inclusión en programas de estudio:* El Salvador estipula que el Ministerio de Educación incluya en los planes y programas de estudio de educación formal para los niveles inicial, parvulario, básico y medio, contenidos que versen sobre la importancia democratizadora de la transparencia, el derecho de acceso a la información pública, el derecho a la participación ciudadana para la toma de decisiones y el control de la gestión pública y el derecho a la protección de datos personales.
- *Reparación integral en la garantía de habeas data:* Ecuador determina que las sentencias positivas que reconozcan derechos deberán contener, no solo la reparación económica sino la reparación integral de los derechos transgredidos.

2. El caso ecuatoriano y el modelo latinoamericano de protección de los datos Personales

Latinoamérica distingue varias realidades para proteger los datos personales: a) Aquellos países que aún no superan la visión limitada de la intimidad o la privacidad como mecanismo de protección de los datos personales como son: Bolivia, Chile (aunque se está tramitando la aprobación del derecho constitucional desde el año 2018), Honduras, Paraguay, Venezuela y Guatemala;[1543] b) Aquellos que han logrado incorporar al *habeas data* y el derecho, pero que no han logrado plasmarlo en una ley que lo efectivice como: Ecuador; c) Aquellos que han logrado incorporar normativa legal e incluso reglamentaria específica y especializada que desarrolla el derecho constitucional consagrado: Brasil, Perú, Costa Rica, México, Colombia, Nicaragua, Panamá y República Dominicana; d) Normativa legal e incluso reglamentaria específica y especializada que desarrolle el derecho a la protección de datos personales, aun cuando no existe reconocimiento constitucional de este, como el caso de Argentina, y

[1543] Bolivia reconoce solo la acción de protección de la privacidad; Chile que solamente reconoce el derecho a la vida privada; Honduras que consagra el *habeas data* pero basado en la intimidad; Brasil, Paraguay y Venezuela que reconocen la garantía constitucional de *habeas data* centrada en la protección de la intimidad y en la privacidad; y, Guatemala que protege datos personales en bases de datos públicos, aunque mediante jurisprudencia de la Corte de Constitucionalidad se garantiza protección a datos personales en ficheros privados pero basado en la intimidad personal, la privacidad y el honor.

Uruguay; y e) Normativa dispersa de carácter sectorial como el caso de Bolivia, Ecuador, Honduras, El Salvador, Paraguay, Guatemala y Cuba.

En el caso del Ecuador, se incorpora al *habeas data* en la Constitución del año 1996, mientras que el derecho fundamental a la protección de datos personales se consagra en la Constitución de 2008. Junto con Perú (1993), Nicaragua (*habeas data* 1995) (derecho 2014), Panamá (2002) y República Dominicana (2010) son el grupo de países que en un primer momento incorporaron esta acción en sus normas constitucionales, y posteriormente reconocieron el derecho fundamental.

Mientras que países como España y Colombia reconocen al menos dos tipos de derechos jerárquicamente diferenciados: los constitucionales y los fundamentales, siendo estos últimos los que conforme dicha distinción son los únicos que tienen la posibilidad de exigir su protección mediante amparo o tutela.[1544] Para la mayoría de las Constituciones latinoamericanas los derechos tienen el mismo rango y, por tanto, gozan de igual protección. En consecuencia, es posible interponer el *habeas data* como garantía constitucional en Latinoamérica.

De otro lado, otros países se decantaron por acciones distintas al *habeas data* como Colombia (1991) mediante la acción de tutela, Argentina mediante la acción de amparo (1994) y de México, por medio de la Ley de Amparo modificada en 2016, a través de la acción de amparo. No obstante, estos tres países han desarrollado normativa específica que ha logrado proteger el derecho fundamental.

Lamentablemente, de la lista de países señalada, Ecuador, Venezuela y Bolivia no han desarrollado normativa especializada que materialice el derecho y permita establecer un sistema preventivo de protección, además del reactivo de carácter constitucional existente.

Dicho de otra manera, no se han establecido garantías primarias o sustanciales, que son aquellas obligaciones o prohibiciones que tienen por presupuesto asegurar la efectividad de un derecho constitucional, ya que establecen acciones y omisiones que deben ser realizadas, tanto por los poderes públicos como por los particulares con la finalidad de que la protección de los derechos sea efectiva. Generalmente, dichos preceptos se encuentran en normativas, por lo que la generación de leyes específicas puede considerarse como garantías primarias. Precisamente, esta es la deficiencia existente en los citados países: la ausencia de normativa especializada que proteja tanto desde la perspectiva preventiva como reactiva. Esto revela la insuficiencia de las garantías secundarias por sí solas, pues se activan una vez que las garantías primarias han sido inefectivas o violadas.[1545] En otras palabras, cuando los preceptos normativos son incumplidos, son los órganos judiciales los llamados a sancionar o anular actos violatorios de derechos constitucionales, para lo cual se han interpuesto previamente acciones o garantías como el *habeas data*.

La ausencia de normativa legal supone una laguna que afecta la efectividad del derecho, pero que también propicia la ausencia de otras de las consecuencias naturales de la vigencia de una norma: las funciones preventiva y reguladora. En tanto que, quienes manejen datos no buscan a priori vulnerar derechos, sino que deben ser regulados con la finalidad de que el tratamiento

[1544] C. STORINI, "Las garantías constitucionales de los Derechos Fundamentales en la Constitución Ecuatoriana de 2008", en *La Nueva Constitución del Ecuador: Estado, derechos e instituciones* (Quito: Corporación Editora Nacional, 2009), 287-8.
[1545] L. FERRAJOLI, "Garantías constitucionales", *Revista Argentina de Derechos Constitucionales* (2000).

cumpla con estándares que les permita un ejercicio de sus actividades apegado a derecho y por ende la protección de los ciudadanos que están detrás de los datos procesados. En consecuencia, "Si no existe ley, deberán evitar el perjuicio al derecho aplicándolo en su contenido esencial. Si existe ley y tienen dudas sobre su constitucionalidad, deberán acudir a la Corte Constitucional".[1546]

Adicionalmente, Ecuador no ha desarrollado suficiente jurisprudencia sobre *habeas data* (existe unas pocas resoluciones que fueron analizadas en el primer capítulo de este trabajo) que orienta la aplicación del derecho a la protección de datos personales, por lo que tampoco esta ha sido una opción posible para viabilizar su aplicación.

Pese a lo limitada de la protección de los datos personales en Ecuador, se ha señalado que existe un elemento innovador en el reconocimiento de la garantía de *habeas data* que debe ser reconocido y resaltado, el cual fue analizado en el primer capítulo de este trabajo investigativo, que se refiere a la reparación integral.

Así, la Constitución ecuatoriana de 2008 incorpora a la reparación integral en el artículo 86 y la vuelve aplicable a todas las garantías constitucionales existentes, entre las cuales consta el *habeas data*. En este sentido, el numeral tercero del citado artículo 86 expresamente incluye como obligación de los jueces que, al momento de dictar sentencias, debe ordenarse la reparación integral material e inmaterial del derecho lesionado. Esto significa que dicha sentencia debe especificar e individualizar las obligaciones, positivas y negativas del destinatario de la decisión judicial y las circunstancias en que dichas obligaciones deban cumplirse, que no pueden limitarse a la reparación económica, sino que deben propiciarse la reparación de los daños inmateriales e incluso dictarse otras formas de reparación propias del sistema de defensa de derechos humanos, como son las medidas de satisfacción y las garantías de no repetición.

Finalmente, en el primer capítulo de este trabajo se realizó un análisis pormenorizado de la situación ecuatoriana y el capítulo final plantea una propuesta normativa de solución que pueda ser discutida por la Asamblea Nacional y de ser el caso promulgada como Ley de la República; para lo cual, la determinación de los elementos del contenido esencial de cada uno de los países latinoamericanos analizados es insumo fundamental porque permite comprender el alcance y las precisiones de este modelo de protección.

Es decir, identificar contenidos mínimos; precisiones; desarrollos propios, ajenos al modelo europeo, contradicciones, confusiones y dificultades prácticas que permitan desarrollar un proyecto de ley para el Ecuador, apto y aplicable, incluso para la región.

3. Conclusiones

Luego del análisis de los veinte y dos países latinoamericanos, incluido Ecuador, se colige que los datos personales en Latinoamérica se protegen de forma heterogénea, ya que El Salvador, Venezuela, Bolivia, Chile, Honduras y Paraguay lo hacen desde una perspectiva acotada a la intimidad. Mientras que Puerto Rico, Jamaica y Haití lo hacen desde la visión de la *privacy* anglosajona.

[1546] L. PRIETO SANCHIS, *Justicia constitucional y derechos fundamentales* (Madrid: Trotta, 2009), 439.

Argentina, Brasil, Colombia, Costa Rica, Ecuador, Guatemala, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay consagran en el ámbito constitucional o legal el derecho a la protección de datos personales.

Es característica propia del sistema latinoamericano el reconocimiento de un mecanismo de tutela o de garantía constitucional denominado *habeas data*. Su reconocimiento inicial estuvo en Brasil en el año 1988, así como en la mayoría de Constituciones de la región como la de Paraguay en 1992, Perú en 1993, Ecuador en 1996, Venezuela en 1999, Panamá en 2002, Honduras en 2003, República Dominicana en 2010 y Nicaragua, en el 2014.

Otros países optaron por otras garantías constitucionales como la tutela en el caso de Colombia en el año 1991. Argentina lo hizo por medio del subtipo de amparo constitucional o *habeas data* constitucional en 1994. Bolivia consagró inicialmente al *habeas data* para, luego, derogar esta garantía constitucional y consagrar otra denominada acción de protección de la privacidad.

El Salvador, Bolivia, Chile, Honduras, Paraguay y Venezuela si bien reconocen el *habeas data*, lo hacen desde el derecho a la intimidad. Mientras que los otros países de la región: Argentina, Brasil, Colombia, Costa Rica, Ecuador, Guatemala, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay, al reconocer a nivel constitucional o legal el derecho a la protección de datos personales, ampliaron el ámbito de cobertura del *habeas data* que también se aplica a la protección de datos personales e incluso a otros derechos fundamentales.

Además, en Argentina, Brasil, Colombia, Costa Rica, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay se ha dictado normativas especializadas de protección de datos personales que establecen sistemas preventivos y reactivos de atención, que al mismo tiempo que regulan los flujos informacionales también protegen derechos de sus titulares.

En consecuencia, en Latinoamérica aún se debaten temas superados como el contenido esencial propio del derecho a la intimidad y el derecho a la protección de datos personales.

Respecto de la intimidad, como se analizará oportunamente, a escala mundial este derecho tiene un origen privado e individualista, porque históricamente solo ostentaban intimidad aquel que tenía propiedades donde generar un espacio privado[1547] como consecuencia de la generalizada burguesía de la segunda mitad del siglo XIX convertida en clase social dominante. La Declaración Universal de los Derechos Humanos proclamada por la Asamblea General de la ONU, del 10 de diciembre del 1948, incluye por primera vez a la intimidad como un derecho fundamental. El artículo 12 de la mencionada declaración señalaba que: "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias y ataques". Es decir, propiedad e intimidad se separan. Intimidad deja de ser un derecho perteneciente a una clase social con un sentido patrimonial y se constituye un derecho autónomo e independiente que protege al individuo, principalmente, de las intromisiones arbitrarias.

Con similar proceso evolutivo, el derecho a la protección de datos personales tiene en la intimidad sus antecedentes inmediatos. No obstante, es mediante la definición de su contenido esencial que se ha construido un derecho diferente basado, sobre todo, en la autodeterminación informativa.

[1547] A.M. BENDICH, Privacy, Poverty and the Constitution, en vol. *Conference on the Law of the poor* (Berkeley: University of California, 1966), 7, accedido 16 de junio del 2007 http://links.jstor.org/sici?sici=0008-1221(196605)54%3A2%3C407%3APPATC%3E2.0.CO%3B2-9

En consecuencia, el derecho a la protección de datos personales en Latinoamérica no fue concebido, inicialmente, como un derecho fundamental autónomo, independiente, complejo e instrumental de origen jurisprudencial, como ocurrió en Europa; sino que ha sido incorporado sobre la base de reformas constitucionales y legales marcadas por la influencia europea.

De otro lado, Latinoamérica al reconocer al *habeas data* como garantía constitucional se alejó de la visión anglosajona, que protege la *privacy* de las personas mediante normativas básicas como *Privacy Act*, o de regulaciones propias del libre mercado y por medio de la autonomía de la voluntad de las partes.

Latinoamérica marca su impronta mediante el *habeas data* en sus diversas variantes, anotándose que esta garantía constitucional protege no solo la autodeterminación informativa, sino otros derechos fundamentales relacionados con la intimidad, el honor, la identidad, la información, entre otros.[1548]

Para Roberto Cesario:

> La acción de hábeas data ha sido reconocida no sólo en las legislaciones de muchos países sino que también por parte de organismos internacionales, los que han elaborado pautas para contribuir a la integración de la perspectiva con la que debe ser evaluada la modalidad de sus ejercicios, e indica como ejemplos las directrices que han formulado la ONU, OEA, Consejo de Europa y Corte Europea de Derechos Humanos.[1549]

Si bien, inicialmente, la protección de los datos de carácter personal en Latinoamérica tomó su propio rumbo, debido a la incorporación constitucional del *habeas data*. Que marcaba una posición intermedia entre la posición anglosajona de control de los datos personales mediante la *privacy* y la consagración de un derecho fundamental autónomo, el derecho a la autodeterminación informativa.

Sin embargo, paulatinamente los países latinoamericanos se han acercado más al modelo europeo. En primer lugar, porque van en la misma línea evolutiva de reconocimiento inicial desde la primigenia intimidad al evidente reconocimiento de la autodeterminación informativa, y del derecho a la protección de datos personales. Esto debido a que es insuficiente un sistema basado en lo íntimo frente a las evidentes transgresiones que suscitan por los avances tecnológicos que ponen en mayor riesgo a los individuos, de tal forma que ha debido consagrar este derecho en sus Constituciones o en sus leyes el derecho a la protección de datos personales.

En segundo lugar, porque la doctrina y la jurisprudencia han reconocido la inexistencia de mecanismos ordinarios de protección de los derechos relacionados con la libertad informática,[1550] y más aún que la acción de tutela a pesar de su especial importancia en

[1548] PUCCINELLI, *Tipos y subtipos*.
[1549] R. CESARIO, *Hábeas data: Ley 25,326* (Buenos Aires, 2001).
[1550] Sobre la inexistencia de una regulación comprensiva del poder informático, y la insuficiencia de los mecanismos de protección actualmente vigentes, la Corte se ha pronunciado en repetidas ocasiones. Así, en las sentencias T-414 de 1992, SU-082 de 1995, T-307 de 1999 entre otras. En esta última, frente al problema de la insuficiencia de los mecanismos de protección, afirmó: "estos mecanismos resultan algunas veces insuficientes para la garantía plena, pronta y efectiva de los derechos comprometidos en el proceso informático. En efecto, no sólo se trata de garantías *ex post*, que no establecen *ab initio* reglas claras para todas las partes comprometidas en este proceso, sino que muchas veces no tienen el alcance técnico que se requiere para lograr la verdadera protección de todos los bienes e intereses que se encuentran en juego."

materia de protección de los derechos; es decir, el *habeas data* y la intimidad no constituyen herramientas suficientes para la reconducción adecuada de las conductas desarrolladas en el ámbito del poder informático.[1551]

En el mismo sentido, se ha afirmado que los:

> [...] recursos de hábeas data no son más que instrumentos o mecanismos de garantía procesal que se acuerdan a favor de las personas que han sufrido una lesión en su ámbito de intimidad producto de usos abusivos de sus datos o informaciones. Se trata, en general, entonces, de un derecho procesal reactivo frente a una lesión ya ocasionada. No tienen una vocación preventiva de las lesiones y sus efectos son casi siempre acordados a favor del afectado y no tienen efectos extensivos hacia quienes sufren las mismas lesiones. Es curioso, y este es un fenómeno que merece mayor estudio e investigación, que en el ámbito latinoamericano la gran evolución hacia leyes de tutela se haya convertido en una mera reglamentación del hábeas data, el cual, en teoría, depende más bien del desarrollo de la jurisprudencia de tutela que vayan sentando los tribunales constitucionales, la cual, en el caso de Costa Rica, ha sido cada vez más generosa. Este avance de la jurisprudencia nacional en materia de hábeas data hace conservar la esperanza de que, tarde o temprano, podremos contar con un estándar de tutela reactivo de indudable importancia. No obstante, al igual que en otros países, aún es necesario acordar tutelas preventivas, que reaccionen antes de que se ocasionen riesgos de incalculables proporciones para una gran cantidad de ciudadanos.[1552]

En tercer lugar, ha influido la postura europea que determina que solo intercambiará datos personales y mantendrá relaciones con aquellos países declarados con niveles adecuados. Estrategia que ha motivado a varios países latinoamericanos a adaptarse en los ámbitos legal y funcional como son los casos de Argentina y Uruguay.

En consecuencia, es acertada la posición de varios países latinoamericanos que determina que, además de reconocer la garantía constitucional de *habeas data*, también se debe consagrar el derecho fundamental a la protección de datos personales.

Asimismo, el *habeas data* ha evolucionado de tal manera que debe velar por las múltiples dimensiones de los datos en relación con los derechos a la autodeterminación informativa y, por ende, protección de datos personales; así como respecto de otros derechos como el de la intimidad, imagen y propia voz, honor, buen nombre, identidad, entre otros.

Ha quedado rezagada la postura acerca de considerar que la acción constitucional constituye en sí misma el reconocimiento de este derecho; prueba de ello es la actual aprobación por parte de la Cámara de Diputados (pendiente únicamente la aprobación por parte del Presidente de la República) de la normativa chilena que modifica la Constitución en esta materia.

Es evidente la necesidad que el nivel de protección de los datos personales no se limiten al reconocimiento del derecho constitucional o de su garantía, sino que deben consagrarse normativas especializadas:

> Dada la necesidad de proteger efectivamente y de manera categórica el derecho a la autodeterminación informática, la Corte considera indispensable que se establezcan normas

[1551] Corte Constitucional de Colombia, "Sentencia T-729/02", cit.

[1552] Ley de Protección de la Persona frente al tratamiento de sus datos personales 8968, 7 de julio de 2011, Asamblea Legislativa de la República de Costa Rica.

> sobre la obligación de adoptar los mecanismos de seguridad adecuados, que permitan la salvaguardia de la información contenida en las bases de datos. Se requieren normas que establezcan sanciones y regímenes especiales de responsabilidad para las entidades administradoras de bases de datos y para los usuarios de la información, así como normas dirigidas a desestimular y sancionar prácticas indebidas en ejercicio del poder informático: cruce de datos, divulgación indiscriminada, bases de datos secretas, entre otras. Por último, también son indispensables normas que regulen los procesos internos de depuración y actualización de datos personales, así como los de las solicitudes de rectificación, adición y supresión de los mismos.[1553]

Resulta importante definir el contenido esencial del derecho a la protección de datos personales, con la finalidad de identificar si la normativa constitucional o legal latinoamericana establece límites razonables o suficientemente justificados. Es decir, si existen limitaciones que aunque cuenten a su favor con buenas razones, resulten ilegítimas y por ende llegaren a dañar el contenido mínimo o esencial del derecho. Esta doble garantía del contenido esencial viene siendo requerida en línea de principio por el Tribunal Constitucional español desde su primer pronunciamiento al respecto, la sentencia 11/1981 de 8 de abril sobre el derecho de huelga.[1554]

En ese sentido, cabe citar lo señalado por la Corte Constitucional de Colombia sobre que:

> [...] con el fin de que se pueda establecer el equilibrio[1555] correspondiente entre los derechos a la información y a la autodeterminación informática, es necesario que el acceso a la información personal debidamente administrada se realice bajo dos principios, llamados a operar bajo la premisa de la posición de garante[1556] de la entidad administradora y del peticionario: el principio de responsabilidad compartida, según el cual, tanto quien solicita la información como quien la suministra, desarrollen su conducta teniendo en cuenta la existencia de un interés protegido en cabeza del titular del dato. Y el principio de cargas mutuas, según el cual, a mayor información solicitada por un tercero, mayor detalle sobre su identidad y sobre la finalidad de la información...[1557]

Tal como señala Remolina Angarita "Son disímiles las formas como en los diferentes países se ha constitucionalizado el tema en cuestión."[1558] Es evidente que buena parte de los países latinoamericanos en su conjunto no se encuentran preparados para afrontar los avatares que la implementación de tecnologías emergentes y las posibles transgresiones que pudieran causar a los derechos fundamentales de las personas respecto de sus datos personales, especialmente

---

[1553] Corte Constitucional de Colombia, "Sentencia T-729/02".

[1554] PRIETO SANCHIS, *Justicia constitucional*, 439.

[1555] Sobre la posibilidad de armonización de los derechos a la información y a la autodeterminación informática e intimidad, en la sentencia T-097 de 1995 la Corte afirmó: "El funcionamiento de los bancos de datos y archivos informáticos que corresponde al derecho de toda persona a emitir y recibir informaciones (Artículo 20 C.P.) no es incompatible con el respeto a los derechos fundamentales de las personas a quienes se refieren los datos ni con la efectiva aplicación de los preceptos que los garantizan."

[1556] La posición de garante tiene origen en el nivel de riesgo que apareja la actividad de las administradoras de datos personales, lo que se traduce en términos de la Corte, en un "deber de especial diligencia" asociado al deber de garantizar el respeto a la dignidad humana y los derechos fundamentales a la libertad, buen nombre y honra de los titulares de los datos Así, en sentencia T-414 de 1992. En un sentido similar se pronunció la Corte en la sentencia T-1085 de 2001, caso en el cual, ante el peligro de la negligencia en la actualización de la información que tiene la virtud de viciar de parcialidad los reportes, se impone una "mayor diligencia" de las administradoras de datos.

[1557] Corte Constitucional de Colombia, "Sentencia T-729/02".

[1558] N. REMOLINA ANGARITA, *Aproximación constitucional de la protección de datos personales en Latinoamérica*, Revista Internacional de Protección de Datos Personales, vol. 1, Facultad de Derecho de la Universidad de los Andes, 2012, fecha de consulta en https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf.

en la recogida, tratamiento y cesión de datos. Prueba de ello, es que solo dos países latinoamericanos han sido declarados de nivel adecuado desde el espectro europeo.

Podemos concluir entonces que Latinoamérica debe implementar una serie de acciones que le permitan efectivizar un sistema de protección de los datos personales. En suma, hacer efectivas tanto las garantías primarias como secundarias que materialicen el derecho en la realidad y que permitan generar un cambio cultural de respeto de los datos personales. Dicho de otro modo, realizar varias de las siguientes iniciativas:

a) Incluir el derecho fundamental en aquellas constituciones en las que todavía no se lo reconoce.
b) Legislar de forma específica y dictar leyes de protección de datos, así como homogeneizar estos contenidos en las leyes sectoriales para evitar antinomias.
c) Apuntalar el *habeas data* como acción constitucional abierta a la protección de datos personales y a otros derechos fundamentales.
d) Crear instancias administrativas u organismos especializados dedicados a la protección del derecho y a la difusión y concientización del mismo. Así como, el fortalecimiento de las instituciones existentes y que velan por el cumplimiento de la normativa vigente.
e) Cooperación y colaboración entre órganos de protección para compartir experiencias pero sobre todo para la persecución extraterritorial de responsabilidades en el uso inadecuado de datos personales.
f) Desarrollar políticas públicas en favor del ejercicio de los derechos ARCO, pero en especial respecto del desarrollo de un empoderamiento en la autodeterminación informativa, una cultura de protección y seguridad de los datos personales, con énfasis en grupos vulnerables como niños, niñas y adolescentes; mujeres; y, adultos mayores.
g) Promoción de los derechos y obligaciones y ventajas del uso adecuado de datos personales para ciudadanos, empresas, entidades, públicas, privadas, nacionales e internacionales como mecanismo de difusión y garantía del derecho.
h) Apoyo y promoción en la creación de organismos de la sociedad civil que permitan una participación de todos los actores en el establecimiento de una sociedad de la información respetuosa de los derechos humanos en línea.
i) Impulso al desarrollo de profesionales multidisciplinarios para proteger los datos personales.
j) Búsqueda de la adhesión al Convenio 108 de Europa, única normativa internacional de carácter vinculante sobre la temática.
k) Necesidad de que los países empiecen procesos de mejoras reales para obtener categorías de nivel adecuado de protección no solo por la necesidad de comerciar con Europa sino por generar un espacio homogéneo de protección de la dignidad humana en línea.
l) Desarrollo de regulaciones internacionales o normativas regionales que permitan una misma línea de defensa del derecho en las Américas.
m) Incentivo a la innovación y creatividad con respeto a la privacidad por diseño y por defecto.

Latinoamérica debe lograr una paulatina armonización de las diferentes normativas que permitan una adecuada protección de los datos de carácter personal en la región, para lo cual, existen iniciativas propuestas por organismos internacionales mediante el Informe de la Relatoría Especial para la Libertad de Expresión, la Corte Interamericana de Derechos Humanos, la Organización de Estados Americanos, la Organización de las Nacionales Unidas

y la Red Iberoamericana de Protección de Datos Personales, los cuales propugnan estándares o directrices que pretenden orientar la emisión de normativas en aquellos países donde aún no se dictan leyes específicas, pero además que determinan referentes de actualización para aquellas que deben acompasarse con las realidades tecnológicas existentes.

Finalmente, es imperioso que Latinoamérica comience a construir un frente único, armónico y eficiente emulando al europeo, por medio de organismos regionales como la Comunidad Andina de Naciones o el Mercosur, pues solo mediante este tipo de iniciativas, de posturas conjuntas se podrá promover una cultura de protección de datos y garantizar una protección adecuada de las personas y un libre flujo informacional que garantice el desarrollo económico, social y cultural de nuestros países.

Sobre cuestiones específicas relacionadas con el contenido esencial que han sido analizadas a lo largo de este trabajo comparándolas con las condiciones generales de la región, además de su utilidad como insumo para el desarrollo de una propuesta normativa para el Ecuador, también resulta útil desde la perspectiva de identificar las brechas en los distintos temas.

Esto por cuanto, al no tener una normativa común que pueda establecer un estándar único para los países latinoamericanos se ha podido identificar:

a) Legislaciones de aquellos países cuya brecha es alta debido a que su nivel de protección aún se ancla en la intimidad como derecho (El Salvador, Venezuela, Bolivia, Chile, Honduras y Paraguay)
b) Legislaciones de aquellos países en los que existe normativa constitucional o legal sobre protección de datos personales pero debido a diversas situaciones no pueden alcanzar un estándar de protección adecuado desde la visión del mayor exponente de protección, Europa, a través del RGPD (Brasil, Colombia, Costa Rica, Ecuador, Guatemala, México, Nicaragua, Panamá, Perú, República Dominicana).
c) Legislaciones de aquellos países en los que existe normativa constitucional o legal sobre protección de datos personales y que debido a la fortaleza de sus sociedad e instituciones de control han podido ser declarados como países con nivel adecuado (Uruguay y Argentina)

Entonces, a través del análisis realizado de cada uno de los elementos del contenido esencial que se puede identificar brechas y campos de mejora, es decir que principios, derechos, obligaciones y precisiones deben ser incorporados o modificados en las legislaciones de protección de datos existentes que permitan una adecuada protección de datos personales, pero sobre todo afrontar los nuevos retos tecnológicos asociados a *big data*, inteligencia artificial, hiperconexión, internet de las cosas, 5G, *blockchain*, entre otros.

EPÍLOGO

CONTENIDOS ESENCIALES DE UNA LEY PROTECCIÓN DE DATOS PERSONALES PARA ECUADOR

Una vez que se ha descifrado y delimitado el contenido esencial del derecho a la protección de datos personales en los modelos europeo, norteamericano y latinoamericano, el objetivo final de esta investigación consiste en proponer aquellos elementos básicos e indispensables que deben constar en un proyecto de Ley de Protección de Datos Personales, a fin de garantizar una norma con contenido completo, coherente, uniforme y que asegure una tutela efectiva de la dignidad de los ecuatorianos frente al tratamiento de sus datos personales.

1. Realidad del derecho a la protección de datos en Ecuador

A continuación, se realizará un análisis sobre la realidad fáctica del uso de los datos personales en Ecuador.

1.1 Realidad ecuatoriana

En Ecuador yace como práctica arraigada la realización de sorteos para los cuales se solicita de forma presencial, telefónica o por medio de promociones en cadenas de comercio, datos personales que después serán usados para finalidades completamente distintas a las insinuadas inicialmente. También es común la oferta de premios, regalos o cenas que captan a futuros clientes, a los que se les exige portar su tarjeta de crédito para adquirir productos, de negarse a pagar en muchos casos les cobran las supuestas recompensas y en varios otros puede incluso llegar a existir maltrato. Varias personas han denunciado estas acciones abusivas, evidenciándolas incluso como fraude porque aseguran que firmaron documentos para retirar un supuesto agasajo y resultó que firmaban un *voucher* de consumo. Todo ello se produce porque existen bases de datos personales que se usan para vender o promocionar la adquisición de bienes o servicios ya sea por medios físicos o por medios telemáticos. Ni en los documentos escritos, ni en los contactos telefónicos o electrónicos existe un espacio disponible para registrar la voluntad del titular de entregar los datos, menos aún se transparenta el motivo de la recolección, ni los propósitos para los cuales se utilizará la información. De igual modo, es común recibir publicidad escrita, virtual y telefónica no solicitada. Además, es abrumador el crecimiento del *telemarketing* que interrumpe jornadas laborales ofreciendo una gran diversidad de productos, esto motiva a no contestar números desconocidos ante la gran posibilidad de que sean promociones u ofertas de productos.[1559]

Es evidente que en Ecuador existe un mercado negro de base de datos personales; se comercializan incluso mediante páginas de comercio electrónico. En este sentido, se han presentado denuncias penales que actualmente se encuentran en proceso de indagación previa para investigar hechos fácticos del delito y los responsables[1560].

[1559] "Ecuador no tiene ley para proteger datos personales", *El Universo*, 29 de abril de 2018, https://www.eluniverso.com/noticias/2018/04/29/nota/6736146/ecuador-no-tiene-ley-proteger-datos-personales.
[1560] Interceptación ilegal de base de datos. Proceso N° 170101818064001. Fiscalía N° 3 – Unidad para Descubrir Autores, Cómplices y Encubridores. Denunciante DINARDAP, Denunciado Desconocido. Quito-

Cesiones de datos personales no aprobadas por sus titulares entre bancos y aseguradoras, que han propiciado cobros indebidos por servicios no autorizados han producido un reclamo generalizado de la sociedad ante la falta de controles en distintos niveles que revelan atentados contra los derechos de los consumidores, cuenta ahorristas o usuarios de la banca, así como titulares de datos personales.[1561]

De otro lado, la sociedad ecuatoriana y el Estado también han sufrido la ausencia de esta normativa con varios sucesos que han causado conmoción social como el producido el 31 de octubre de 2017, en donde, tras un operativo realizado en Santo Domingo de los Tsáchilas se logró determinar que personas inescrupulosas se hicieron pasar por beneficiarios del Bono de Desarrollo Humano y cobraron 8.000.000 (ocho millones) de dólares indebidamente, haciendo uso inadecuado de los datos personales que contenía una base del Ministerio de Inclusión Económica y Social.[1562]

Asimismo, un hecho grave denunciado en el segmento semanal *El Gobierno Informa*, por el propio presidente de la República, Lenin Moreno, el 29 de enero de 2018, por el cual informó a la ciudadanía del robo de la base de datos del Plan Toda una Vida, una base de datos personales sensibles pues incluyen nombres de personas que pertenecen al quintil de pobreza en Ecuador y cuya finalidad era la entrega de beneficios públicos, y que una vez extraída fue usada para enviar "un mensaje malicioso a 400.000 (cuatrocientos mil) ecuatorianos convocándoles a recibir la asignación de una casa". Información falsa que pretendía repercutir de forma negativa en la percepción popular y el apoyo al presidente, y en consecuencia directamente en la consulta popular realizada en ese año .[1563]

En otro hecho, en el mes de marzo de 2018 se denunció que los sistemas de la Agencia Nacional de Tránsito fueron vulnerados; modificándose fraudulentamente la base de datos de la institución, lo que dio como resultado que falsificadores y tramitadores entregaran 15.970 (quince mil novecientos setenta) licencias de conducir de manera ilegal.[1564]

Transgresiones que se evidencian desde tiempo atrás, que no han sido reconocidas como un atentado al derecho a la protección de datos personales, por ejemplo, en el 2014 se denunció, por parte de un ciudadano, ante la Defensoría del Pueblo del Ecuador que el Banco de Machala negó la creación de una cuenta de ahorros al individuo, debido a que constaba dentro de la base de datos de personas indiciadas, procesadas y sentenciadas por ilícitos

---

Ecuador. Revelación ilegal de bases de datos. Proceso N° 170101818060469. Fiscalía de Soluciones Rápidas N° 2. Denunciante DINARDAP, Denunciado Desconocido. Quito-Ecuador. Revelación ilegal de bases de datos. Proceso N° 170101819072102. Fiscalía de Soluciones Rápidas N° 7. Denunciante DINARDAP, Denunciado DataBook. Quito-Ecuador. Revelación ilegal de bases de datos. Proceso N° 170101819100071. Fiscalía de Soluciones Rápidas N° 3. Denunciante DINARDAP, Denunciado Novaestrat. Quito-Ecuador. Acceso no consentido a un sistema informático (base de datos). Proceso N° 170101819110653. Fiscalía de Soluciones Rápidas N° 3. Denunciante DINARDAP, Denunciado Equivida. Quito-Ecuador.

[1561] Expreso.ec, "Débitos no autorizados molestan a los clientes", accedido 24 de octubre de 2018, https://www.expreso.ec/economia/debitos-no-autorizados-molestan-a-los-cliente-NAgr_4581611.

[1562] "$ 8'000.000 del Bono de Desarrollo Humano habrían sido cobrados indebidamente; hay siete detenidos", *El Universo*, accedido 25 de octubre de 2018, https://www.eluniverso.com/noticias/2017/10/31/nota/6459943/8000000-bono-desarrollo-humano-habrian-sido-cobrados-indebidamente.

[1563] "Lenín Moreno denuncia el robo de la base de datos del Plan Toda Una Vida", *El Comercio*, accedido 25 de octubre de 2018, https://www.elcomercio.com/actualidad/leninmoreno-denuncia-robo-basededatos-plan.html.

[1564] "8.582 conductores portan licencias tipo 'B' ilegales", *El Telégrafo*, 28 de marzo de 2018, https://www.eltelegrafo.com.ec/noticias/judicial/12/conductores-licencias-ilegales.

sancionados en la Ley de Sustancias Estupefacientes y Psicotrópicas; base de datos que se encuentra a disposición de todas las entidades bancarias, sin que medie autorización del titular, mandato de ley u orden judicial que habilite su tratamiento.[1565]

La alta exposición de las problemáticas personales en redes sociales también supone un riesgo por la entrega masiva de datos personales consecuencia de esta. De ello resultan más vulnerables los niños, adolescentes e incluso adultos mayores, quienes no son del todo conscientes de los riesgos que asumen en el manejo de estas herramientas.

El 16 de septiembre de 2019, tras un informe de los investigadores de ZDnet y VPNmentor, expuestos en sus blogs respectivamente, se reveló la filtración de los datos de 20 millones de ecuatorianos, incluso de aquellos que habían fallecido hasta la fecha; en donde se evidenciaba que tras la falta de incorporación de medidas de seguridad a los servidores, ubicados en Miami, de Novaestrat, una empresa ecuatoriana dedicada al análisis de datos, se exponían nombres, correos electrónicos, números de teléfono, estado civil, datos bancarios, de automóviles, entre otros, dentro de los cuales se incluía información de 6.7 millones de niñas, niños y adolescentes, datos sensibles, como género o número de cuentas bancarias, así como datos detallados de familiares del titular de la información, como dirección de residencia, números de seguros y cédulas[1566]

Existe una marcada falta de interés hacia reclamar este tipo de agresiones a la dignidad, debido al desconocimiento de las personas respecto de la entidad responsable de atenderle, el tipo de trámite y las reales consecuencias de iniciar estos procesos. Además, media el gasto desmesurado que presentan estas acciones penales y de otras que no llegan a revestir condiciones de antijuridicidad suficiente para convertirse en delito, pero que son afectaciones al consumidor y que, al considerarse de bagatela, tampoco son objeto de reclamo.

Sumado a esto, acciones de *habeas data* que no prosperan, para defensa de derechos, sino que se decantan por soluciones procesales o limitadas a acceso y rectificación de datos en sus respectivas bases —como se analizó en el capítulo primero de este estudio— y no sobre la verificación de si se están produciendo valoraciones automatizadas o brechas de seguridad que pudieran afectar la integridad del ser humano titular del dato.

En suma, se visibiliza a la sociedad ecuatoriana como inconsciente de sus derechos, ignorante del contenido esencial de la protección de datos personales, y pese a que presiente que algo es incorrecto y no funciona de manera adecuada, desconocedora de los riesgos que el uso indiscriminado de sus datos puede acarrear no solo a sí mismos, en sus derechos de la personalidad como intimidad, imagen, honor u honra, sino de otros derechos que en virtud de valoraciones automatizadas o datos erróneos constantes en bases podrían impedir su acceso a la vivienda, trabajo, educación, salud, entre otros.

Ejemplos palpables de esta realidad se suscitan cuando una condición de deudor equivocada consta plasmada en una base de datos, y el ciudadano común no logra identificar el mecanismo que le permita borrar ese dato erróneo y peor aún, consecuencia de estos deslices,

[1565] Defensoría del Pueblo. Resolución N° DPE-DGT-DNAPD-16-2014-DO, *CONSEP*, Trámite N° DPE-DGT-DNAPD-133-2013-DO, 22 de diciembre de 2014.
[1566] "BBC revela filtración de datos sensibles de millones de ecuatorianos", *El Comercio*, accedido 25 de septiembre de 2019, https://www.elcomercio.com/tendencias/datos-ecuatorianos-filtracion-reporte-seguridad.html

se han iniciado trámites coactivos que podrán repercutir en su economía a tal punto de impedirle acceso a créditos o afectar incluso su remuneración.

1.2 Insuficiencia y contradicciones de la legislación ecuatoriana sobre protección de datos personales

Como se analizó en el primer capítulo de la presente tesis, en el año 2008 Ecuador consagró como derecho fundamental el de la protección de los datos personales; sin embargo, diez años después, no se ha promulgado una norma que desarrolle su contenido.

No obstante, en Ecuador los derechos constitucionales son de aplicación directa al tenor de lo dispuesto en el artículo 11 numeral 3 de la Constitución que señala:

> Art. 11.- El ejercicio de los derechos se regirá por los siguientes principios: [...] 3. Los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte. Para el ejercicio de los derechos y las garantías constitucionales no se exigirán condiciones o requisitos que no estén establecidos en la Constitución o la ley.
>
> Los derechos serán plenamente justiciables. No podrá alegarse falta de norma jurídica para justificar su violación o desconocimiento, para desechar la acción por esos hechos ni para negar su reconocimiento.

Sin embargo, el contenido, alcance, dimensión y forma de eficacia de estos derechos no puede ser materializado por la ausencia normativa. Tampoco la jurisprudencia ecuatoriana ha desarrollado los elementos necesarios para su operatividad como son los derechos, los principios, las obligaciones, las infracciones y las sanciones.

En consecuencia, es obligación de la Asamblea Nacional dictar una norma que viabilice la vigencia efectiva del derecho; así como de la Corte Constitucional la de dictar resoluciones que definan los matices de este derecho. La única resolución vinculante emitida por la Corte Constitucional,[1567] que analiza el derecho a la protección de datos personales y las cuestiones procedimentales del *habeas data*, es la sentencia 001-2014-PJO-CC, expedida en el 2014. En ella, se analizan en los *obiter dicta* varias temáticas como el derecho a la autodeterminación informativa, y la comprensión del concepto de dato personal, pero en la *ratio decidendi* se limita a temas procedimentales del *habeas data* y no aborda temáticas fundamentales como la necesidad de establecer principios de tratamiento que garantice el derecho, por ejemplo. Por tanto, tampoco la jurisprudencia ha podido disponer de un sistema de protección jurisprudencial, como se ha intentado en otros países, como El Salvador o Paraguay.

Lamentablemente ninguna de estas dos posibilidades de regulación se ha cumplido en estos diez años desde la vigencia de la Constitución de Montecristi. Además, se ha avanzado muy poco en regulaciones de nivel inferior, en resoluciones de autoridad pública o jurisprudencia del ámbito ordinario que determinen un marco de aplicación mínimo para la vigencia de este

[1567] Corte Constitucional del Ecuador, "Sentencia 001-2014-PJO-CC", Gaceta Constitucional n.º 007, 7 de marzo de 2014.

derecho, lo que hace que sobre este tema exista un espacio de desprotección que debe corregirse.

Si bien existe normativa sectorial, que en algo pretende poner en práctica la disposición constitucional, lejos de aclarar el alcance del derecho a la protección de datos personales, demuestra lo dispersa, contradictoria e incompleta que es |nuestra legislación en esta temática. Incluso una parte de ella se encuentra desactualizada, porque está asociada a la visión inicial de salvaguarda anclada en la intimidad que imperaba en la Constitución de 1998, como ocurre con el artículo 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; o es de aplicación exclusivamente restrictiva a ciertos ámbitos específicos, como las normas contenidas en la Ley de Telecomunicaciones o el Código Orgánico Integral Penal.

Adicionalmente, el sistema de protección de datos personales en Ecuador se limita entonces a la garantía constitucional del *habeas data*. La problemática de este sistema es que la garantía jurisdiccional, si bien evita transgresiones directas mediante los derechos de acceso, rectificación, cancelación y oposición, no permite proteger otros derechos que pueden verse conculcados. Aunque se han dictado varias resoluciones relativas a *habeas data*, como se concluyó en el primer capítulo de esta investigación, esta garantía constitucional presenta una evidente limitación: solo procede ante un posible daño o un daño producido. Es decir, la tutela es limitada a una protección post, cuando existen serias presunciones o ya se ha producido una transgresión y no establece un sistema de prevención, que recoja principios, derechos y obligaciones que deben cumplirse para un adecuado manejo de los datos personales y que en conjunto eviten que se produzcan posibles daños.

De otro lado, han existido pocas iniciativas y de poco impacto para presentar y discutir proyectos de ley en esta temática. La Asamblea Nacional, en tres ocasiones fallidas, ha intentado discutir un proyecto de ley.

En el año 2010 se planteó el denominado "Proyecto de Ley de Protección a la Intimidad y Datos Personales", propuesta del asambleísta Bethoven Chica que fue desestimado en el año 2013, tras recomendación de la Comisión Especializada Permanente de Justicia y Estructura del Estado debido a que su contenido planteaba una visión asociada a la intimidad.

Conviene decir que esta confusión entre derecho a la intimidad y derecho a la protección de datos personales se encuentra ampliamente superada por la propia Constitución de 2008 que los consagra en numerales distintos, por su contenido autónomo e independiente, y ámbito de cobertura diferente. El derecho a la protección de datos personales, si bien nace de la intimidad debido a que se creía que solo era aplicable a la recopilación de datos íntimos en bases informáticas, ahora tiene contenido propio basado en la autodeterminación informativa que empodera al titular para que bajo su decisión se entregue o no datos personales a responsables para su tratamiento. El avance de la tecnología y de la ciencia de datos conlleva no solo abusos en el almacenamiento de los datos en bases públicas o privadas, sino que se violente la información de las personas, incluso en la recogida de información.

De modo que la protección de datos personales comienza a independizarse y a encontrar autonomía respecto de otros derechos, en la medida en la que encuentra un elemento de titularidad y de desarrollo de la personalidad, al descubrir que tenemos una identidad digital y que esta se encuentra almacenada en bases de datos o que, debido a los actuales mecanismos de perfilamiento, puede ser generada incluso de forma automatizada. Aunque debe

considerarse que esta información puede estar desactualizada, ser equívoca, e indebidamente tratada para finalidades ajenas a las cuales fue recabada.

En cualquiera de esas situaciones existe la posibilidad de vulnerar derechos fundamentales. Entonces, el derecho a la protección de datos personales se aparta de la intimidad, debido a que para violentar a la persona no es preciso que exista una agresión a la esfera íntima del individuo; es decir, no se necesita que los datos sean íntimos, pues el derecho a la protección de datos personales ampara al individuo, y como este determina su información en el mundo real y en el mundo virtual, incluso con datos que pudieran considerarse irrelevantes o inocuos, pero que en conjunto construyen un perfil completo de la personalidad.

El ex presidente de la Función de Transparencia y Control Social durante el año 2013, Fabián Jaramillo Palacios, también máxima autoridad de la Superintendencia de Telecomunicaciones, desarrolló el proyecto de "Ley de Protección de Datos y Privacidad", que no se volvió público y tampoco prosperó, debido a la promulgación de la Ley Orgánica de Telecomunicaciones en Registro Oficial, de 18 de febrero de 2015 que eliminó este órgano de control.

En 2016 se presentó la "Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales", por la entonces presidenta de la Función Legislativa, Gabriela Rivadeneira. La Dirección Nacional de Registro de Datos Públicos y varias organizaciones civiles han presentado reparos a esta propuesta, solicitando su archivo. Se ha informado a la Asamblea que la citada Dirección se encuentra desarrollando un proyecto de ley que recoja los principales avances del contenido de este derecho y, además, se adapte a la realidad ecuatoriana.[1568]

En todos los casos planteados, la falta de conocimientos técnicos ha derivado en la discusión de estos textos en el plano político con temáticas completamente ajenas al derecho a la protección de datos personales, como la transparencia, la libertad de expresión, el control de redes sociales. Esto se debe a que en estas propuestas normativas se incluyeron normas no compatibles con el derecho. Además, se equivocaron argumentos de discusión, o se omitió evidenciar realidades ecuatorianas que motiven su promulgación; por el contrario, se optó por transcripciones de legislaciones de otros países,[1569] con absurdas adaptaciones que trastocaron el contenido de este derecho a tal punto de equivocadamente proponer el derecho a la intimidad y privacidad sobre los datos personales, como en el caso del texto propuesto en el 2016.[1570]

En ese escenario la tarea del legislador, del ejecutivo y de la función jurisdiccional se vuelve indispensable, pues todos en conjunto deben ir construyendo paulatinamente los alcances, límites y contornos de este derecho en cada ámbito en el que se aplique. Solamente un sistema adecuado de prevención y control, una clara determinación de los derechos de los titulares, de los principios y de las obligaciones que deben cumplir los responsables de las

[1568] "DINARDAP cuestionó el proyecto de Ley de Protección de los Derechos a la Intimidad que analiza la Asamblea Nacional – Datos Públicos", accedido 9 de septiembre de 2018, http://www.datospublicos.gob.ec/dinardap-cuestiono-el-proyecto-de-ley-de-proteccion-de-los-derechos-a-la-intimidad-que-analiza-la-asamblea-nacional/.
[1569] Ibíd.
[1570] "Gabriela Rivadeneira: 'En ningún momento ley restringirá datos de funcionarios públicos'", *El Comercio*, 16 de septiembre de 2016, https://www.elcomercio.com/actualidad/gabrielarivadeneira-ley-datospersonales-ecuador-asamblea.html.

bases de datos, la generación de una institucionalidad propia y de mecanismos de disuasión coercitivos pueden brindarnos un entorno normativo que viabilice el ejercicio de este derecho.

En este contexto, la Dirección Nacional de Registro de Datos Públicos ha tomado a bien trabajar, desde el mes de noviembre de 2017, el Anteproyecto de Ley Orgánica de Protección de Datos Personales, basándose en un proceso de construcción participativa, en donde todos los actores interesados puedan aportar a la elaboración de una norma de alto impacto a nivel nacional e internacional, mismo que fue presentada a través del Ministerio de Telecomunicaciones y Sociedad de la Información, el ente rector en la materia y al que la DINARDAP se encuentra adscrita, a la Asamblea Nacional del Ecuador, el 19 de septiembre de 2019.

Parte del proceso de elaboración normativa ha sido la construcción de una cultura de protección de datos personales, para lo cual se trabajó en una campaña de difusión tanto del derecho en sí mismo, como del proceso de elaboración del proyecto de ley y de los beneficios de esta normativa para el Ecuador. Como evidencia de este trabajo consta cada una de las referencias periodísticas con su correspondiente link de acceso en el Anexo 2.

1.3 Normativa sectorial sobre protección de datos personales en Ecuador

Con la finalidad de verificar la normativa dispersa que debe ser tomada en cuenta para elaborar un sistema uniforme para la protección de los datos personales, a continuación se analizará la normativa vigente relacionada con la temática y las posibles contradicciones o incomprensiones que deben solucionarse mediante disposiciones finales, transitorias o normas reformatorias o derogatorias. Las citadas normativas son:

1.3.1 Ley de Comercio Electrónico, Firmas y Mensajes de Datos[1571]

El artículo 9 de la Ley de Comercio Electrónico y Firmas Electrónicas establece que:

> Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

[1571] Ecuador, *Ley 67, Ley de Comercio Electrónico, Firmas y Mensajes de Datos*, Registro Oficial Suplemento 577, 17 de abril de 2002.

Por cuanto la Ley de Comercio Electrónico, Firmas y Mensajes de Datos es del año 2002, cuando aún estaba vigente la Constitución de 2008, se confunden los datos personales con datos íntimos. En este sentido, esta norma debe ser modificada eliminando la frase "La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República", y sustituirla por una que diga: "La recopilación y uso de datos personales garantizará los derechos a la protección de datos personales, a la intimidad, la confidencialidad, derecho al honor, a la imagen y a la propia voz, a las libertades individuales y otros derechos fundamentales garantizados por la Constitución de la República del Ecuador, así como permitirá e incentivará el libre flujo informacional".

Debido a que esa norma regula de manera muy simple, además de incompleta, lo relativo al consentimiento y la revocatoria de este y lo atinente a la recopilación de datos personales, es menester modificar en esta parte también la cita mediante el siguiente texto: "Respecto de la recopilación de datos de fuentes accesibles al público y directamente del titular de los datos personales se estará a lo dispuesto en la ley de la materia".

Por otra parte, el quinto artículo de la presente ley resuelve respecto de los principios de confidencialidad y reserva que su establecimiento se dará "para los mensajes de datos, cualquiera sea su forma, medio o intención", añadiendo que "Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia".

La norma indicada deberá concordar con la determinación de las obligaciones que los responsables y encargados de tratamiento deben cumplir, así como con la descripción y alcance del principio de confidencialidad, de manera que se incluya en el texto estas consideraciones.

En el mismo contexto, la disposición general novena, que atañe al glosario de términos indica respecto del derecho a la intimidad que este "comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados." Así también, propone como datos personales a los "datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley".

Nuevamente, el concepto de derecho a la intimidad está equivocado pues invoca en él consideraciones propias del derecho a la protección de datos personales como lo relativo a los datos proporcionados en cualquier relación contra terceros o su divulgación. En este sentido, esta norma debe acoplarse a lo dispuesto en el artículo 66, numeral 20 de la Constitución de la República del Ecuador.

Finalmente, el concepto de datos personales debe ser eliminado para invocarse directamente lo constante en la Ley de Protección de Datos Personales.

1.3.2 Ley Orgánica de Registro de Datos Públicos[1572]

La Constitución de la República del Ecuador en el artículo 18 determina que todas las personas en forma individual o colectiva tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

Es decir, es derecho de las personas el acceder a información pública. Por su parte, el artículo 227, de la norma *ibídem,* establece que "La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación". Ahora bien, el Estado no solo almacena datos públicos sino también datos personales que por disposición de la ley deben incluirse en registros públicos, con la finalidad de cumplir con principios como el de publicidad registral, seguridad jurídica y que permiten materializar derechos como el de propiedad, libertad de comercio y empresa, trabajo, entre otros.

Para regular, organizar y sistematizar los registros públicos, en Suplemento del Registro Oficial 162, del 31 de marzo de 2010, entró en vigencia la Ley Orgánica[1573] del Sistema Nacional de Registro de Datos Públicos, por la cual se creó y reguló el Sistema Nacional de Registro de Datos Públicos, en entidades públicas o privadas que administren dichas bases o registros; y su correspondiente entidad responsable, esto es la Dirección Nacional de Registro de Datos Públicos (Dinardap).

La Ley Orgánica del Sistema Nacional de Registro de Datos Públicos tiene como objetivo regular los registros públicos que manejan las entidades públicas o privadas, garantiza, organiza y normaliza la seguridad jurídica, de forma eficiente y eficaz. Para lo cual maneja adecuadamente la transparencia, publicación, accesibilidad a las nuevas tecnologías, relacionadas con el uso de datos en el ámbito registral. Esta ley es aplicable a las instituciones privadas o públicas, que manejen los registros públicos, ya sean de personas naturales o jurídicas. Esta información será entregada de forma general o específica, por escrito o a través de medios electrónicos.

Asimismo, según el artículo 28 de la norma *ibídem*, el Sistema Nacional de Registro de Datos Públicos tiene por finalidad "proteger los derechos constituidos, los que se constituyan, modifiquen, extingan y publiciten por efectos de la inscripción de los hechos, actos y/o contratos determinados por la presente Ley y las Leyes y normas de registros; y con el objeto de coordinar el intercambio de información de los registros de datos públicos".

[1572] Ley 0, Registro Oficial Suplemento (en adelante, ROS) 162, 31/mar/2010, *Ley del Sistema Nacional de Registro de Datos Públicos*.
[1573] Mediante Ley S/N publicada en el Segundo Suplemento del Registro Oficial 843, 3 de diciembre de 2012, se dio el carácter de Orgánica a la Ley del Sistema Nacional de Registro de Datos Públicos.

De ese modo, la Ley del Sistema Nacional de Registro de Datos Públicos establece entre una de sus prioridades la creación de un sistema unificado de datos públicos registrables; es decir, el registro de datos respecto de los bienes o patrimonio de las personas naturales o jurídicas por parte de las instituciones del sector público y privado que actualmente o en el futuro administren bases o registros de datos públicos. Esta inscripción, respecto de la titularidad de derechos reales asociados a persona o personas determinadas, tendría como finalidad la de plasmar el modo de adquirir el dominio y otros derechos reales de los bienes raíces mediante la denominada *tradición*; de contribuir a dar publicidad de los actos y contratos en garantía de los derechos de terceros; y de garantizar la autenticidad y seguridad de los títulos, instrumentos públicos y documentos.

El artículo 31, numeral 5 de la norma *ibídem*, establece como atribución de la Dirección Nacional de Registro de Datos Públicos la de "Consolidar, estandarizar y administrar la base única de datos de todos los Registros Públicos, para lo cual todos los integrantes del Sistema están obligados a proporcionar información digitalizada de sus archivos, actualizada y de forma simultánea conforme ésta se produzca".

El artículo 13, de la norma *ibídem*, prescribe que:

> La Dirección Nacional de Registro de Datos Públicos, de conformidad con la ley, expedirá las normas técnicas que contengan los estándares, mecanismos y herramientas para precautelar la seguridad, custodia y conservación de la información accesible y confidencial. La integridad y protección de los registros de datos públicos es responsabilidad de las instituciones del sector público y privado, a través de sus representantes legales y las personas naturales que directamente los administren.

La Ley Orgánica de Transparencia y Acceso a la Información Pública en el artículo 5 determina que "Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado".

El artículo 10 de la ley *ibídem* establece que:

> Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción. Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, pérdida y/o desmembración de documentación e información pública.

El artículo cuarto de dicha ley responde a la responsabilidad de la información al mencionar que:

> [...] las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este proveen toda la información. Las personas afectadas por información falsa o imprecisa, difundida o certificada por registradoras o registradores, tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de la respectiva acción legal. La Dirección Nacional de Registro de Datos Públicos establecerá los casos en los que deba rendirse caución.

La Ley del Sistema Nacional de Registro de Datos Públicos, que rige a la Dinardap, está encaminada a garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información entre las instituciones que integrar el Sistema Nacional de Registro de Datos Públicos (Sinardap); sin embargo, en dicha ley no existe una definición de lo que es un dato público ni su clasificación, lo cual lleva a revisar su reglamento que señala lo siguiente:

En la disposición general séptima: "4. Datos públicos.- Exclusivamente en el ámbito de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, se entenderá como datos públicos, a todo acto y/o información relativa a las personas naturales o jurídicas, sus bienes o patrimonio, sean estos accesibles o confidenciales, generadas del sector público o privado". Esta norma, en particular, debe ser reformada para adaptarla a los conceptos analizados en este trabajo de investigación.

De igual manera define en el numeral 10, de la disposición general séptima, la protección de datos como "el procedimiento determinado por la Dirección Nacional de Registro de Datos Públicos para definirla accesibilidad o confidencialidad de los datos, con la finalidad de proporcionar protección jurídica".

No obstante, la legislación ecuatoriana no cuenta con una ley especializada en protección de datos personales, lo cual ha conllevado a que la Dinardap adopté en parte como base jurídica las leyes antes citadas para emitir resoluciones que, de cierta manera pretenden establecer parámetros encaminados al tratamiento de datos en las instituciones que forman parte del Sinardap, así como el establecer conceptualizaciones muy generales las cuales no desarrollan la nueva visión de protección de datos, derecho que se encuentra muy avanzado normativamente a nivel regional e internacional. Por ejemplo, la Dinardap emitió la resolución 039-NG-DINARDAP-2016, denominada "Norma que establece el procedimiento para la integración de entes registrales, fuentes externas y fuentes internas en el sistema nacional de registro de datos públicos". En el artículo 3 da la misma definición de la protección de datos que consta en el reglamento: "El procedimiento determinado por la Dirección Nacional de Registro de Datos Públicos para definir la accesibilidad o confidencialidad de los datos, con la finalidad de proporcionar protección jurídica".

Esta misma resolución hace una clasificación de los datos públicos, desde la perspectiva de establecer los parámetros para clasificar la información que es administrada por la Dinardap y no desde un enfoque que permita garantizar la protección de datos como un derecho fundamental. Así, establece datos de carácter accesible, confidenciales y datos públicos, siendo el concepto de datos confidenciales el que más se acerca a una conceptualización de datos personales.

En la resolución 035-NG-DINARDAP-2016, denominada "Norma que regula la clasificación de los datos que integran el sistema nacional de registro de datos públicos", se define a los datos o información de carácter personal como "toda información no pública correspondiente a la persona, por medio de la cual se la pueda identificar, contactar o localizar, entre otras", pero teniendo el enfoque para el tema de clasificación de datos públicos enmarcados en la interoperabilidad.

Dentro de las resoluciones antes citadas, se evidencia que la protección de los datos se limita solamente al tema de *interoperabilidad*, definida en la disposición general séptima, numeral 9, del Reglamento a la Ley del Sinardap, como "el intercambio y uso de información entre dos o más sistemas, aplicaciones o componentes tecnológicos" entre instituciones públicas que forman parte del Sinardap. Esta normativa solo está orientada para la clasificación de datos, como un acto previo a la entrega de la información a las otras instituciones a fin de que estas presten un servicio público a la ciudadanía.

Por eso, es pertinente analizar la Ley del Sistema Nacional de Registro de Datos Públicos (en adelante LSNRDP). Esta ley tiene por objeto diseñar, implementar, administrar y regular el sistema de registro de datos públicos para conformar una base de datos única de toda la información registral concerniente a personas naturales y jurídicas; también garantizar seguridad jurídica, sistematizar e interconectar la información mediante las nuevas tecnologías[1574] y proveer de información válida a la sociedad ecuatoriana.[1575]

Son parte del sistema quienes actualmente o en el futuro administren bases o registros de datos públicos, por ejemplo: a) las dependencias públicas, desconcentradas, con autonomía registral y administrativa como: Registro Civil, de la Propiedad, Mercantil, Societario, Vehicular, de naves y aeronaves, patentes, de propiedad intelectual, registros de datos crediticios y los que en la actualidad o en el futuro determine la Dirección Nacional de Registro de Datos Públicos;[1576] b) las instituciones del sector privado; y también, c) las personas usuarias de los registros públicos.[1577]

[1574] Ley 0, Registro Oficial Suplemento (en adelante, ROS) 162, 31/mar/2010, *Ley del Sistema Nacional de Registro de Datos Públicos*. "Art. 1.- Finalidad y Objeto.- La presente ley crea y regula el sistema de registro de datos públicos y su acceso, en entidades públicas o privadas que administren dichas bases o registros.
El objeto de la ley es: garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información, así como: la eficacia y eficiencia de su manejo, su publicidad, transparencia, acceso e implementación de nuevas tecnologías."

[1575] Dirección Nacional de Registro y Datos Públicos del Ecuador, "Planificación Estratégica 2015-2017", 2015, http://www.datospublicos.gob.ec/wp-content/uploads/downloads/2016/02/PLANIFICACI%C3%93N-ESTRAT%C3%89GICA-2015-2017.pdf.

[1576] Ley 0, ROS 162,31/mar/2010, *Ley del Sistema Nacional de Registro de Datos Públicos*. **"**Art. 13.- De los registros de datos públicos.- Son registros de datos públicos: el Registro Civil, de la Propiedad, Mercantil, Societario, Vehicular, de naves y aeronaves, patentes, de propiedad intelectual registros de datos crediticios y los que en la actualidad o en el futuro determine la Dirección Nacional de Registro de Datos Públicos, en el marco de lo dispuesto por la Constitución de la República y las leyes vigentes.
Los Registros son dependencias públicas, desconcentrados, con autonomía registral y administrativa en los términos de la presente ley, y sujetos al control, auditoría y vigilancia de la Dirección Nacional de Registro de Datos Públicos en lo relativo al cumplimiento de políticas, resoluciones y disposiciones para la interconexión e interoperabilidad de bases de datos y de información pública, conforme se determine en el Reglamento que expida la Dirección Nacional".

[1577] Ibíd. "Art. 2.- Ámbito de aplicación.- La presente Ley rige para las instituciones del sector público y privado que actualmente o en el futuro administren bases o registros de datos públicos, sobre las personas naturales o jurídicas, sus bienes o patrimonio y para las usuarias o usuarios de los registros públicos".

Determinados los actores, resta identificar qué tipos de datos forman parte del sistema de registro de datos públicos regulados por esta ley, a fin de determinar si la nomenclatura usada para agrupar este conjunto de datos es la correcta. Así como, determinar si los sistemas de protección previstos en la presente norma son los pertinentes, atendiendo a la naturaleza de cada uno de los datos que lo integran, en especial respecto a los datos personales que son parte de esta base de datos accesible al público.

Se empezará por aquellos de mayor cuidado, los datos denominados sensibles. Pertenecen a este grupo los datos de: "ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales".[1578] En lo que concierne a su acceso, "sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial".[1579]

Cabe añadir que "También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado".[1580]

Por otro lado, aludiendo a la autoridad o funcionario que custodie datos de carácter personal, se menciona que este "deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos".[1581]
E impone una serie de presupuestos para un solicitante frente a su requerimiento de conocer información patrimonial respecto de terceros; en ese contexto "deberá justificar y motivar su requerimiento, declarar el uso que hará de la misma y consignar sus datos básicos de identidad, tales como: nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el/la titular de la información pueda ejercer".[1582] Finalmente, adhiere que "La Directora o Director Nacional de Registro de Datos Públicos, definirá los demás datos que integrarán el sistema nacional y el tipo de reserva y accesibilidad".[1583]

Por lo señalado, los datos que integran el sistema de registro de datos públicos son: a) Aquellos hechos, actos, contratos o instrumentos que deben inscribirse y/o registrarse, en virtud de la aplicación de la ley propia de cada materia;[1584] b) Aquellos datos cuya reserva haya sido declarada por la autoridad competente; c) Datos de carácter personal de aquellos

[1578] Ibíd., artículo 6, LSNRDP.
[1579] Ibíd.
[1580] Ibíd.
[1581] Ibíd.
[1582] Ibíd.
[1583] Ibíd.
[1584] Ibíd. "Art. 3.- Obligatoriedad.- En la ley relativa a cada uno de los registros o en las disposiciones legales de cada materia, se determinará: los hechos, actos, contratos o instrumentos que deban ser inscritos y/o registrados; así como la obligación de las registradoras o registradores a la certificación y publicidad de los datos, con las limitaciones señaladas en la Constitución y la ley.
Los datos públicos registrales deben ser: completos, accesibles, en formatos libres, sin licencia alrededor de los mismos, no discriminatorios, veraces, verificables y pertinentes, en relación al ámbito y fines de su inscripción.
La información que el Estado entregue puede ser específica o general, versar sobre una parte o sobre la totalidad del registro y será suministrada por escrito o por medios electrónicos."

considerados como sensibles referidos a ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales, cuyo acceso es posible únicamente con autorización expresa del titular de la información, por mandato de la ley o por orden judicial; d) Datos amparados bajo sigilo bancario o bursátil; e) Datos que pudieren afectar la seguridad interna o externa del Estado.[1585]

De otro lado, el artículo 4 del Instructivo de clasificación de la información de la Dirección Nacional de Registro de Datos Públicos, Registro de Datos Crediticios y Registros Mercantiles, a efectos de este sistema, toda información que es administrada, recibida, generada, transmitida y almacenada en las instituciones que la conforman, se clasifica en información pública,[1586] información confidencial,[1587] y esta a su vez en reservada[1588] y secreta.[1589] Sin embargo, los conceptos aquí delineados confunden información con

[1585] Ibíd. "Art. 6.- Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales.
El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial.
También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado.
La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos.
Para acceder a la información sobre el patrimonio de las personas el solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará de la misma y consignar sus datos básicos de identidad, tales como: nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el/la titular de la información pueda ejercer.
La Directora o Director Nacional de Registro de Datos Públicos, definirá los demás datos que integrarán el sistema nacional y el tipo de reserva y accesibilidad."

[1586] "Artículo 5.- Información Pública.- Para los efectos de la presente norma, se considera Información Pública a todo documento físico y digital que emane, administre o se encuentre en poder de la DINARDAP, Registros Mercantiles y Registro de Datos Crediticios, que está sujeta al principio de publicidad". Instructivo de clasificación de la información de la Dirección Nacional de Registro de Datos Públicos, Registro de Datos Crediticios y Registros Mercantiles, Resolución 043-NG-DINARDAP-2016 (Registro Oficial 899, 9-XII-2016).

[1587] "Artículo 6.- Información Confidencial.- Es aquella información o conocimiento que no está sujeta al principio de publicidad, la cual es accesible únicamente a personal autorizado, de conformidad con lo establecido por el ANEXO 2 de esta norma, misma que será declarada como tal, por la máxima autoridad de la Dirección Nacional de Registro de Datos Públicos, de conformidad con lo establecido por el inciso sexto, del artículo 6 de la Ley del Sistema Nacional de Registro de Datos Públicos". Instructivo de clasificación de la información de la Dirección Nacional de Registro de Datos Públicos, Registro de Datos Crediticios y Registros Mercantiles, Resolución 043-NG-DINARDAP-2016 (Registro Oficial 899, 9-XII-2016).

[1588] "Artículo 6.- Información Confidencial.- [...] a) Información Reservada.- Se entiende a aquella que no es de libre acceso, pero que se pudiere otorgar el mismo, si los funcionarios de cada área, o de otras instituciones o terceros interesados, justifican legalmente el menester de tener acceso a la misma.
Por norma general, los datos de carácter personal administrados tanto por la DINARDAP, como de sus entidades adscritas, son considerados como reservados". Instructivo de clasificación de la información de la Dirección Nacional de Registro de Datos Públicos, Registro de Datos Crediticios y Registros Mercantiles, Resolución 043-NG-DINARDAP-2016 (Registro Oficial 899, 9-XII-2016).

[1589] "Artículo 6.- Información Confidencial.- [...] b) Información Secreta.- Es aquella información o conocimiento cuya divulgación puede poner en riesgo o comprometer la existencia de un bien jurídico de orden económico, social, de salud, de gobernabilidad, de seguridad, o amenace la prevención, investigación y sanción

documentos y no mencionan el término dato lo que además de una omisión evidente no permite comprender el alcance de la norma; esto es si solo opera para la organización de los registros públicos o si es aplicable al cruce de información o la interoperabilidad. Adicionalmente, no guardan armonía con los conceptos que constan en otras normativas sobre la misma temática como la Ley Orgánica de Transparencia y Acceso a la Información Pública, la Ley de Seguridad Pública y del Estado y el Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público que se analizarán en su momento.

Finalmente, el artículo 3 de la LSNRDP menciona el concepto de datos públicos registrales al señalar que estos deben ser completos, accesibles, en formatos libres, sin licencia alrededor de los mismos, no discriminatorios, veraces, verificables y pertinentes; además, deberán ser publicitados, con las limitaciones señaladas en la Constitución y la ley.

Por tanto, es necesario identificar la naturaleza jurídica de los datos públicos registrales con la finalidad de no confundirlos: ni con el concepto de datos personales ni con el de datos públicos. De este modo, los registros públicos están conformados por datos personales y datos públicos, por lo que deben ser entendidos como datos públicos registrales y datos personales registrales, respectivamente. Pues la registrabilidad es la característica de, por voluntad de la ley, estar incorporada o registrada en un registro público o base de datos de registro público, para la generación de efectos jurídicos como la transferencia de dominio o la adquisición de derechos y obligaciones, en virtud de garantizar derechos y principios como el derecho de identidad, derecho de propiedad, derecho de libertad de comercio y empresarial, entre otros, y de los principios de publicidad, accesibilidad y el de seguridad jurídica.

Cabe anotar que, por constar en un registro público, los datos personales o los datos públicos no modifican su naturaleza jurídica primigenia, por lo que el dato personal, por ejemplo, no se transforma ni muta en dato público por el hecho de que conste en un registro público. Únicamente se vuelve accesible al público en virtud de la necesidad de hacer disponible este dato en satisfacción de intereses legítimos de terceros.

1.3.3 Ley Orgánica de Telecomunicaciones[1590]

El artículo 78 de la Ley Orgánica de Telecomunicaciones, al referirse a la protección de datos personales, señala:

> Para la plena vigencia del derecho a la intimidad, establecido en el artículo 66, numeral 20 de la Constitución de la República, las y los prestadores de servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de datos de carácter personal.

---

de las infracciones establecidas en la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos. La información clasificada como secreta, será entregada únicamente por orden judicial o cuando el uso de la misma sea imperativo para factores de auditoría, control y vigilancia de la autoridad competente". Instructivo de clasificación de la información de la Dirección Nacional de Registro de Datos Públicos, Registro de Datos Crediticios y Registros Mercantiles, Resolución 043-NG-DINARDAP-2016 (Registro Oficial 899, 9-XII-2016).

[1590] Ecuador, *Ley Orgánica de Telecomunicaciones*, ROS 439, 18 de febrero de 2015, https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Orgánica-de-Telecomunicaciones.pdf

> Para tal efecto, las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus redes con el fin de garantizar la protección de los datos de carácter personal de conformidad con la ley. Dichas medidas incluirán, como mínimo:
>
> 1. La garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley.
>
> 2. La protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos.
>
> 3. La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.
>
> 4. La garantía de que la información suministrada por los clientes, abonados o usuarios no será utilizada para fines comerciales ni de publicidad, ni para cualquier otro fin, salvo que se cuente con el consentimiento previo y autorización expresa de cada cliente, abonado o usuario. El consentimiento deberá constar registrado de forma clara, de tal manera que se prohíbe la utilización de cualquier estrategia que induzca al error para la emisión de dicho consentimiento.

Esta norma reconoce el derecho a la protección de datos personales, y determina su aplicación en el ámbito de las telecomunicaciones, al señalar elementos como la seguridad, el consentimiento, la finalidad; hace alusión a un sistema de control y vigilancia que lamentablemente no es supervigilado por el organismo de control especializado. De lo citado, la norma debe ampliarse o en su caso hacer remisión expresa a las disposiciones de una Ley de Protección de Datos Personales para que el régimen de protección sea completo y no fraccionado a los pocos principios abordados.

El artículo 85 de esta ley, al mencionar las obligaciones adicionales dispone que:

> La Agencia de Regulación y Control de las Telecomunicación establecerá y reglamentará los mecanismos para supervisar el cumplimiento de las obligaciones tanto de secreto de las comunicaciones como de seguridad de datos personales y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para las y los prestadores de servicios, con el fin de que adopten determinadas medidas relativas a la integridad y seguridad de las redes y servicios.

Estipula además que entre las medidas constarán: "1. La obligación de facilitar la información necesaria para evaluar la seguridad y la integridad de sus servicios y redes, incluidos los documentos sobre las políticas de seguridad. 2. La obligación de someterse a costo del prestador, a una auditoría de seguridad realizada por un organismo público, autoridad competente o, de ser el caso, por una empresa privada o persona natural independiente."

Finalmente, debería evitarse que la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador (Arcotel) realice las funciones de órgano de control sobre estas temáticas, pues no es el organismo técnico especializado, sino que debería serlo una Superintendencia de Protección de Datos Personales.

1.3.4 Ley Orgánica de Transparencia y Acceso a la Información Pública (Lotaip)[1591]

En el sexto artículo de la Lotaip se propone como información confidencial a "aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales" para en lo posterior sumar que "el uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes". Se concluye con que "no podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno", exceptuando "el procedimiento establecido en las indagaciones previas".

De lo citado, la frase información pública personal causa confusión, porque el término público no hace alusión a información estatal, sino a publicidad o accesibilidad al público. En tal sentido, información confidencial es aquella información pública o información personal que por motivos legítimos debe ser resguardada del conocimiento de otros. En el caso de la información personal, por esencia es confidencial, por lo que la ley debe establecer los casos en los que se justifica sea accesible al público por parte de terceros, lo que generalmente debe ser proporcional y basado en un interés legítimo de quien busca acceder a esta información.

1.3.5 Código Orgánico Monetario y Financiero[1592]

El artículo primero de este Código establece el objetivo principal: regular "los sistemas monetario y financiero, así como los regímenes de valores y seguros del Ecuador", [1593] ya que, por medio de normas, control, supervisiones y redición de cuentas de las actividades realizadas, se generan sistemas de inspección. Se procura que estos procedimientos vayan acordes a la ley.[1594] El artículo 152 habla de los derechos de las personas naturales o jurídicas. El conocer su información de forma clara, precisa y no engañosa, se reconoce como un derecho importante. Los datos personales que consten en entidades financieras deberán ser exactos y actualizados, conforme la ley lo disponga, porque estos sirven para generar reportes crediticios de los sujetos que consten en su base.[1595]

Ahora bien, la Ley Orgánica PARA EL Fomento Productivo, Atracción de Inversiones, Generación de Empleo, y Estabilidad y Equilibrio Fiscal (ROS 309, 21 de agosto de 2018) estableció que será la Superintendencia de Bancos la que regula el Registro de Datos Crediticios y realice la administración de la base de datos crediticios, creando reportes de forma exacta y actualizada. Esta información es vital para la toma de decisión en créditos que se puedan otorgar a futuro.[1596]

[1591] Ecuador, *Ley Orgánica de Transparencia y Acceso a la Información Pública*, ROS 337, 18 de mayo de 2004.
[1592] Ecuador, *Código Orgánico Monetario y Financiero*, ROS 215, 22 de febrero de 2006.
[1593] Ibíd.
[1594] Ibíd.
[1595] Ibíd.
[1596] Ibíd.

Entretanto, el Código Orgánico, Monetario y Financiero menciona la protección de la información, la cual se establece en el artículo 352 que ampara los datos personales, que se encuentran dentro del sistema financiero nacional. Los titulares de los datos serán los únicos habilitados para acceder a su información, a excepción de lo dispuesto en este Código.

En el mismo sentido, lo dispuesto en el artículo 13 de la Codificación Superintendencia de Bancos[1597] que menciona dentro de los derechos del usuario:

> a. Exigir información y documentación de todos los actos que respalden la negociación, contratación, ejecución y terminación del contrato, y/o de la prestación de productos y servicios financieros ya sea al obligado directo o indirecto; b. Derecho a obtener los documentos que han sido debidamente cancelados o endosados por haberse subrogado en la obligación en calidad de obligado indirecto; y, c. Conocer si en las bases de datos de las entidades de los sectores financieros público y privado existe información sobre sí mismo y acceder a ella sin restricción alguna; a conocer la fuente de dicha información; y, a exigir de la misma la rectificación de los datos personales cuando dicha información sea inexacta o errónea.

Por otra parte, la codificación ya aludida propone en el artículo 14 que "El usuario tendrá derecho a recibir protección y a demandar la adopción de medidas efectivas que garanticen la seguridad de las operaciones financieras, del defensor del cliente, de la Superintendencia de Bancos o de otras instancias administrativas o judiciales pertinentes"; expone principalmente las siguientes circunstancias:

a. Recibir protección ante la existencia de cláusulas prohibidas que vayan en contra de sus derechos e intereses;

b. Recibir protección de los datos personales que las entidades financieras obtengan del usuario para la prestación de productos o servicios financieros. La información sobre dichos datos personales solo podrá ser otorgada por la entidad de los sectores financieros público y privado, en caso de consentimiento libre y expreso, especifico, inequívoco e informado, por parte del usuario, de disposición judicial o del mandato de la ley;

c. Recibir protección de los datos personales que las entidades financieras obtengan del usuario para la prestación de productos y servicios financieros prestados por vía electrónica. Las entidades financieras adoptarán específicamente las medidas de seguridad necesarias para este tipo de operaciones financieras;

d. Obtener protección de los datos personales sobre su solvencia patrimonial y crediticia, y a que las entidades financieras respeten las normas relativas al sigilo y reserva;

e. Exigir rectificación de la información de los datos personales en las bases de datos cuando ésta sea inexacta o errónea;

f. Demandar protección cuando las entidades financieras empleen métodos de cobranza extrajudicial que atenten contra su privacidad, dignidad personal y/o familiar;

[1597] Ecuador, *Codificación Superintendencia de Bancos*, publicada por Codificación Superintendencia de Bancos n.º 810, ROS 123, 31 de octubre de 2017.

g. Exigir que se mantenga la validez de las ofertas financieras. Las condiciones incluidas en los contratos tendrán fuerza vinculante si llegan a efectuarse con base en ellas;

h. Formar y participar en asociaciones para la defensa de los derechos del usuario del sistema financiero, y acudir al defensor del cliente en defensa de sus derechos; y,

i. Demandar la cobertura del fondo de garantía de depósitos, de acuerdo con la ley.

1.3.6 Código Orgánico Integral Penal[1598]

El artículo 229 del Código Orgánico Integral Penal determina el delito de revelación ilegal de base de datos por el cual:

> La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

En ese caso el tipo penal no solo está en garantía de la intimidad o la privacidad, sino del derecho a la autodeterminación informativa que es contenido esencial del derecho a la protección de datos personales, por lo que podría añadirse este término en la tipificación citada.

No requiere reforma pero es necesaria su cita para establecer el marco normativo completo en este código del artículo a continuación, constante en el título denominado actuaciones y técnicas especiales de investigación, expreso en el segundo libro del Procedimiento del Código Orgánico Integral Penal. Se dispone en el artículo 472 sobre la información de circulación restringida que: "No podrá circular libremente [...] La información acerca de datos de carácter personal y la que provenga de las comunicaciones personales cuya difusión no haya sido autorizada expresamente por su titular, por la ley o por la o el juzgador".

1.3.7 Ley Orgánica de Salud (LOS)[1599]

La Ley Orgánica de Salud, en el artículo 215, señala que "la autoridad sanitaria nacional con la participación de los integrantes del Sistema Nacional de Salud, implementará el sistema común de información con el fin de conocer la situación de salud, identificar los riesgos para las personas y el ambiente, dimensionar los recursos disponibles y la producción de los servicios, para orientar las decisiones políticas y gerenciales y articular la participación ciudadana en todos los niveles, entre otras".

[1598] Ecuador, *Código Orgánico Integral Penal*, ROS 180, 10 de febrero de 2014.
[1599] Ecuador, *Ley Orgánica de Salud*, ROS 353, 23 de octubre de 2018.

Por eso, no es necesario modificar normativa en dicho Código, sino precisar que la implementación de este sistema común de información deberá cumplir con los derechos principios y obligaciones de una Ley de Protección de Datos Personales, pues se trata de datos personales relacionados con la salud tratados por el Estado, con el Ministerio de Salud como responsable.

De otro lado, la Ley Orgánica de Salud establece la confidencialidad de varios datos de salud que deben ser resguardados desde la perspectiva de una normativa de protección de datos personales, estos son:

a) Enfermedades transmisibles, no transmisibles, crónico-degenerativas, discapacidades y problemas de salud pública declarados prioritarios, y determinar las enfermedades transmisibles de notificación obligatoria (art. 6, num. 5, LOS).

b) La historia clínica (art. 7, LOS).

c) Casos sospechosos, probables, compatibles y confirmados de enfermedades declaradas por la autoridad sanitaria nacional como de notificación obligatoria y aquellas de reporte internacional (art. 61, LOS).

d) Registro e información de pacientes que padezcan enfermedades raras o huérfanas incluidas las residentes en el extranjero que padezcan enfermedades raras o huérfanas, a fin de brindar atención oportuna en el país de residencia y de ser el caso en el territorio nacional (art. 3, LOS).

1.3.8 Código Orgánico de la Economía Social de los Conocimientos, Código Ingenios[1600]

El presente Código, en la disposición general vigésima séptima dispone que "Sin perjuicio de las excepciones previstas en la ley, el tratamiento de datos personales que incluya acciones tales como la recopilación, sistematización y almacenamiento de datos personales, requerirá la autorización previa e informada del titular". Agrega que: "No se requerirá de la autorización del titular cuando el tratamiento sea desarrollado por una institución pública y tenga una finalidad estadística o científica; de protección a la salud o seguridad; o sea realizado como parte de una política pública de garantía de derechos constitucionalmente reconocidos. En este caso deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares. La DINARDAP podrá solicitar que los bancos de datos personales en poder de una persona jurídica privada sean entregados a la misma con la finalidad de cumplir el presente artículo". Finalmente, propone una serie de excepciones:

No se sujetarán a lo prescrito en el presente artículo:

a) Las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico;

b) Las bases de datos y archivos de información periodística y otros contenidos editoriales; y,

[1600] Ecuador, *Código Orgánico de la Economía Social de los Conocimientos*, ROS 899, 9 de diciembre de 2016.

c) Las bases que contengan datos cuyo uso puede atentar a la privacidad de las personas tales como aquellos que revelen la orientación política, las convicciones religiosas o filosóficas, la pertenencia a organizaciones políticas o sociales.

Por otro lado, la disposición general vigésima sexta establece que:

> Las entidades públicas y personas naturales o jurídicas privadas que tengan bajo su poder documentos, datos genéticos, bancos o archivos de datos personales e informes sobre personas o sobre sus bienes, pondrán a disposición del público a través de un portal de información o página web la siguiente información y recursos:
>
> a) Los derechos que le asisten respecto de la protección de sus datos personales, entre ellos el derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos; y sus derechos a solicitar la rectificación, eliminación o anulación de sus datos personales;
>
> b) Detalle de las políticas y procedimientos institucionales para la protección de la privacidad de datos personales; y,
>
> c) Servicio de trámite en línea de las consultas y reclamos en materia de datos personales.

Como mecanismo poco eficiente, se introdujeron estas normas en un Código cuya finalidad es garantizar derechos relacionadas a la economía social de los conocimientos, la creatividad y la innovación. Cuando por tratarse de un derecho fundamental, la protección de datos personales amerita una ley especializada en la cual se pueda garantizar los derechos y libertades individuales y el flujo de información. En este sentido, estas dos normas deben ser eliminadas porque no se justifica su existencia en el citado cuerpo normativo, ni aun a título de sectorial.

1.3.9 Ley Orgánica de Comunicación[1601]

El artículo 30 de la Ley Orgánica de Comunicación, respecto de la información de circulación restringida, sostiene que esta:

> No podrá circular libremente, en especial a través de los medios de comunicación, la siguiente información:
>
> 1. Aquella que esté protegida expresamente con una cláusula de reserva previamente establecida en la ley;
>
> 2. La información acerca de datos personales y la que provenga de las comunicaciones personales, cuya difusión no ha sido debidamente autorizada por su titular, por la ley o por juez competente;
>
> 3. La información producida por la Fiscalía en el marco de una indagación previa; y,

[1601] Ecuador, *Ley Orgánica de Comunicación*, ROS 22, 25 de junio de 2013.

4. La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo establecido en el Código de la Niñez y Adolescencia.
La persona que realice la difusión de información establecida en los literales anteriores será sancionada administrativamente por la Superintendencia de Información y Comunicación con una multa de 10 a 20 remuneraciones básicas mínimas unificadas, sin perjuicio de que responda judicialmente, de ser el caso, por la comisión de delitos y/o por los daños causados y por su reparación integral.

De la cita legal que antecede, por medio de la Ley de Comunicación se intenta controlar la divulgación de datos personales; sin duda es un aporte importante en la construcción de una cultura de protección, en especial de aquellos datos que pertenecen a niños, niñas y adolescentes. Una norma de protección de datos personales se complementaría con la citada dado que condiciona la actuación de los medios de comunicación en aras de proteger a las personas y sus datos.

La mencionada ley también propone en el artículo 13 de su consecuente reglamento con respecto a la protección de la identidad e imagen que esta "no se puede publicar en los medios de comunicación los nombres, fotografías o imágenes o cualquier elemento que permita establecer o insinuar la identidad de niñas, niños y adolescentes que están involucrados de cualquier forma en un hecho posiblemente delictivo o en la investigación y el procesamiento judicial del mismo". Aclara que "La misma prohibición opera para proteger la identidad e imagen de cualquier persona que haya sido víctima de un delito de violencia sexual o violencia intrafamiliar", exceptuando de esta categoría a "los testimonios de personas adultas que voluntaria y explícitamente dan su autorización para que los medios de comunicación cubran sus casos, siempre que esto tenga la finalidad de prevenir el cometimiento de este tipo de infracciones".

Esta norma complementa el sistema que privilegia la protección de datos personales de estos grupos de atención prioritaria; en consecuencia, es valiosa como mecanismo de salvaguarda de los datos personales en el ámbito de las comunicaciones.

1.3.10 Ley Orgánica de Gestión de la Identidad y Datos Civiles[1602]

El artículo 3 de la Ley Orgánica de Gestión de la Identidad y Datos Civiles estipula como objetivos:

1. Asegurar el ejercicio del derecho a la identidad de las personas.

2. Precautelar la situación jurídica entre el Estado y las personas naturales dentro de sus relaciones de familia.

3. Proteger el registro de los hechos y actos relativos al estado civil de las personas.

4. Proteger la confidencialidad de la información personal.

5. Evitar el subregistro o carencia de datos en registro de una persona.

[1602] Ecuador, *Ley Orgánica de Gestión de la Identidad y Datos Civiles*, ROS 684, 4 de febrero de 2016.

6. Proteger la información almacenada en archivos y bases de datos de los hechos y actos relativos al estado civil de las personas.

7. Propender a la simplificación, automatización e interoperabilidad de los procesos concernientes a los hechos y actos relativos al estado civil de las personas, de conformidad a la normativa legal vigente para el efecto.

De los varios propósitos en la normativa citada se colige que por tratarse de un registro público, una ley de protección de datos personales le sería directamente aplicable e impactaría en todos sus ámbitos y procesos; por esto se considera necesario un período de gracia para que puedan adaptarse a su contenido y garantizar el derecho a la protección de datos personales.

1.3.11 Ley de Seguridad Pública y del Estado[1603]

El artículo 19 de la Ley de Seguridad Pública y del Estado señala que los organismos de seguridad y la Secretaría Nacional de Inteligencia pueden realizar la clasificación de la información resultante de las investigaciones o actividades que realicen.
La citada clasificación se deberá realizar mediante resolución motivada de la máxima autoridad de la entidad respectiva, para lo cual el reglamento determinará los fundamentos para la clasificación, reclasificación y desclasificación y los niveles de acceso exclusivos a la información clasificada.

Así, la ley señala que la información y documentación se clasificará como reservada, secreta y secretísima y que será el reglamento el que determine los criterios para la mentada clasificación. En el artículo 28 del Reglamento a la Ley de Seguridad Pública y del Estado[1604] se declarará como información reservada cuando el documento o material que contiene información cuya utilización no autorizada podría perjudicar los intereses organismos de seguridad. Será secreto[1605] si podría ocasionar daño a las instituciones públicas y a los funcionarios que laboran en ellas. Finalmente, se considerará secretísimo cuando podría incidir en un peligro excepcionalmente grave para la seguridad integral del Estado.

El artículo 29 del Reglamento a la Ley de Seguridad Pública y del Estado determina que "Los servidores públicos, ciudadanos civiles y miembros activos de las Fuerzas Armadas y de la Policía Nacional están prohibidos de divulgar información reservada, secreta y secretísima, aún después de cesar en sus funciones".

El artículo 19 de la Ley de Seguridad Pública y del Estado establece que "toda información clasificada como reservada y secreta será de libre acceso luego de transcurridos cinco y diez años, respectivamente; y si es secretísima luego de transcurridos quince años. La información clasificada como secretísima será desclasificada o reclasificada por el Ministerio de Coordinación de Seguridad o quien haga sus veces. De no existir reclasificación, se desclasificará automáticamente una vez cumplido el plazo previsto de quince (15) años".

[1603] Ecuador: *Ley de Seguridad Pública y del Estado*, ROS 352, 8 de septiembre de 2009.
[1604] Reglamento a la Ley de Seguridad Pública y del Estado, Suplemento del Registro Oficial 336, 27 de septiembre de 2018.
[1605] Reformado por el artículo 15 del D.E. 64, RO 36-2S, 14 de julio de 2017.

Por su parte, el artículo 195 del Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público[1606] señala que "Los datos personales de servidoras o servidores que forman parte del servicio, así como las actividades u operaciones que se realicen en función de la misión de la entidad, serán calificados de reservada, secreta o secretísima dependiendo del nivel de confidencialidad que se requiera conforme a la normativa jurídica competente".

De lo transcrito, se desprende que esta clasificación de los datos debe coordinar y ser coherente con el principio de confidencialidad, de tal manera que no exista contradicciones y, por el contrario, la diferente normativa sea armónica, dado que las clasificaciones de reservada, secreta o secretísima no distingue si se trata de datos personales o de datos públicos.

2. Propuesta de Ley de protección de datos personales desde la perspectiva del contenido esencial del derecho

En el mundo existen tres modelos claramente diferenciados: el primero de origen europeo, que reconoce al derecho a la protección de datos personales como un derecho humano de nacimiento jurisprudencial y con corte constitucional, que permite el desarrollo de la personalidad; por eso concibe a los datos de titularidad como un elemento que conforma su personalidad.

El segundo modelo proviene de Estados Unidos y propone a los datos de carácter personal como bienes de propiedad de un individuo o empresa, no como parte de su identidad, ni de su titularidad, sino como manifestaciones externas que puedan ser objetivadas a tal punto que admiten ser transferidos, cedidos, tratados, en la medida en que conformen bases de datos que logren el intercambio de información y recursos económicos en movimiento.

Finalmente, el tercer modelo es el latinoamericano, que toma una postura intermedia entre estas dos posiciones antes señaladas, pues luego de una larga discusión entre intimidad, privacidad y protección de datos personales admiten a este último como un derecho autónomo, y lo vuelve el centro del sistema de salvaguarda de los datos personales. Además, reconoce la figura del *habeas data* como un mecanismo de justicia constitucional que apuntala la protección de las personas en la sociedad red. Esta corriente también toma en consideración ciertas prácticas americanas, como códigos de conductas, prácticas de buena fe y principios de puerto seguro o escudo de privacidad.

Es importante tener en cuenta estos modelos en la medida en que para realizar una propuesta normativa es indispensable identificar cuál es el modelo al que debe apuntar la futura normativa ecuatoriana. ¿Cuál de ellos es el que se compatibiliza de manera general con las fuentes, derechos y principios rectores de la sociedad ecuatoriana y de forma específica que figuras pueden ser adaptadas a nuestra realidad para aprovechar lo mejor de cada modelo en beneficio de los ecuatorianos? En este sentido a continuación se realizará un análisis planteado a la luz de los criterios que han sido usados a lo largo de este trabajo de

[1606] Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público, Suplemento del Registro Oficial 19, 21 de junio de 2017.

investigación como parte del contenido esencial del derecho a la protección de datos personales.

2.1 Objeto

Revisados los modelos de protección de datos personales o privacidad de Europa, Estados Unidos y Latinoamérica, respectivamente, se concluye que el modelo referente para Ecuador es el europeo. A continuación se identificará qué contexto justifica esta postura:

a) *Derecho a la protección de datos personales*. Como se analizó en el capítulo segundo, Europa es la cuna de este derecho cuyas primeras manifestaciones datan del 1 de octubre de 1980, cuando la Organización de Cooperación y Desarrollo Económico dictó la Recomendación del Consejo, relativa a los Flujos Transfronterizos para el Desarrollo Económico y Social. Posteriormente, mediante la jurisprudencia alemana de 1983[1607] se construyen la autodeterminación informativa que, junto a los otros derechos y principios, constituye el derecho a la protección de datos personales, reconocido como derecho humano en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea[1608] y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE).[1609]

Por su parte, Ecuador consagra el derecho a la protección de datos personales en el numeral 19 del artículo 66 de la Constitución de 2008. La decisión sobre el régimen de protección aplicable a los datos personales de los ecuatorianos la tomaron los asambleístas constituyentes cuando incorporaron este derecho en la Carta Magna. Evidencia de lo señalado consta en los debates e informes de discusión de la Asamblea de Montecristi, analizados en el primer capítulo de esta investigación. Se destaca el informe de la Mesa 1 que entre los anexos justificativos incluía una descripción respecto de la naturaleza, derechos, deberes y principios que constituyen y desarrollan este derecho, realizado por Juan Manuel Fernández López, magistrado y ex director de la Agencia de Protección de Datos española.[1610]

Sin duda, la voluntad de la Constituyente de 2008 fue la de reconocer un alto estándar de protección, a diferencia de los otros modelos existentes, esto es el americano limitado a la *privacy* y del latinoamericano, acotado al derecho a la intimidad en el ámbito digital o a la garantía constitucional del *habeas data* como únicos mecanismos de salvaguarda de los datos personales.

Del análisis realizado, se colige que la norma constitucional ecuatoriana incluye los contenidos esenciales de este derecho, toda vez que recoge a la autodeterminación informativa, que se refiere al derecho de las personas a decidir sobre la información que verse

[1607] Sentencia de 15 de diciembre de 1983, BJC núm. 33, IV Jurisprudencia Constitucional Extrajera, 1984.
[1608] Diario Oficial de las Comunidades Europeas, "Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01)", 18 de diciembre de 2000, http://www.europarl.europa.eu/charter/pdf/text_es.pdf.
[1609] "Versión consolidada del Tratado de Funcionamiento de la Unión Europea" (C 83/50 Diario Oficial de la Unión Europea 30.3.2010, s. f.), https://www.boe.es/doue/2010/083/Z00047-00199.pdf.
[1610] M. MOLINA CRESPO, presidenta la Mesa 1 de la Constituyente de 2008, "Informe de la Mesa 1 sobre artículos aprobados para que sean sujetos a discusión de la Asamblea Constituyente de Ecuador de 2008 sobre Derechos Civiles, debido proceso, Derechos Políticos y Derecho a la Comunicación", 6 de mayo de 2008, C-ANCM1-092-08.

sobre sí misma, y al consentimiento del titular o a su vez la autorización de la ley. Asimismo, se describe cada una de las fases del manejo de los datos personales: recolección, archivo, procesamiento, distribución o difusión que luego se decantan en los principios y obligaciones que deben cumplir quienes tratan datos personales y cuyo detalle se desarrolla en leyes y reglamentos que desarrollan derechos constitucionales. Acerca de los derechos ARCO, la norma constitucional usa los términos acceso y decisión; en este último se encuentran inmersos los de rectificación, cancelación y oposición, así como en la siguiente frase del texto constitucional que dice: así como su correspondiente protección.

b) *Respeto a las libertades individuales y derechos fundamentales*. El modelo europeo establece que el tratamiento de datos personales debe protegerse, no solo desde el derecho a la protección de datos personales como derecho inherente, sino que un adecuado manejo de los datos personales en el estado actual de desarrollo tecnológico determina un resguardo a otros derechos como los de vida privada y familiar, domicilio, comunicaciones, protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, derecho a la tutela judicial efectiva y a un juicio justo, a la diversidad cultural, religiosa y lingüística, entre otros, conforme señala el considerando (4) del RGPD. En el mismo sentido, la Corte Constitucional del Ecuador, mediante sentencia 001-14-PJO-CC de 2014, establece que "el derecho a la protección de datos —y específicamente, su elemento denominado 'autodeterminación informativa'—, tiene carácter instrumental, supeditado a la protección de otros derechos constitucionales que se pueden ver afectados cuando se utilizan datos personales". En consecuencia, de los contextos descritos y de los alcances previstos para este derecho, el ámbito de aplicación del modelo europeo resulta asimilable a la realidad ecuatoriana.

c) *Derechos y obligaciones*. Conforme ha señalado el RGPD, que es el referente para el modelo europeo, la protección de los datos personales se materializa mediante la específica estipulación en la normativa legal de los derechos de los titulares y de las obligaciones de quienes tratan o determinan el tratamiento de sus datos; así como, la creación en su momento y el fortalecimiento de las entidades estatales de control que supervisen y garantizar el cumplimiento de las normas y sanciones.[1611]

Por su parte, la normativa constitucional ecuatoriana limita su actuación a las primeras concepciones del modelo latinoamericano, que reconocía como único mecanismo de control la garantía constitucional del *habeas data*, que en el caso del Ecuador consta en el artículo 92 de la Constitución de 2008. Sin embargo, como se analizó en el capítulo cuarto de este trabajo de investigación, esta visión restringida a la protección del derecho desde una perspectiva exclusivamente reactiva —es decir, cuando el daño ya se ha producido— ha sido paulatinamente superada por varios países latinoamericanos que han desarrollado un modelo híbrido. En otras palabras, la vigencia de este sistema de control posterior de rango constitucional y de promulgación de normas especializadas que establecen un marco preventivo y también un administrativo de control por intermedio de autoridades públicas que realizan supervisiones que mejoran los procesos de protección paulatinamente. De modo que la puesta en marcha de los mecanismos de seguimiento y cumplimiento del

[1611] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) Documento DOUE-L-2016-80807, BOE.es, accedido 16 de mayo de 2018, https://www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80807.

derecho se hace desde el ámbito administrativo; solo en aquellos casos en los que el daño y su reparación es inminente se activa la vía judicial.

En consecuencia, Ecuador debe dictar una norma que regule los derechos, principios en el nivel práctico y que incluya a órganos y mecanismos de control que puedan hacer efectiva la vigencia del derecho. Desde esta perspectiva, el modelo continental al que se pertenece Ecuador requiere de normativa legal que establezca un marco completo de protección, por lo que en este sentido tampoco es aplicable el modelo americano, como tampoco normas de conducta voluntarias de las empresas que son figuras que en el *civil law* pueden ser usadas simultáneamente, pero que no son óbice para que una norma de cumplimiento general se establezca.

d) Principio de proporcionalidad. El RGPD estable el principio de proporcionalidad como el mecanismo que permite mantener un equilibrio entre el derecho a la protección de datos personales y otros derechos fundamentales. La Corte Constitucional ecuatoriana es la competente para, en cada caso particular puesto en su conocimiento, aplicar el método de interpretación de los mandatos de optimización, en general mediante la ponderación en sentido lato, conformada por los test de adecuación, test de necesidad y test de proporcionalidad, por los cuales, mediante un sentencia, se determina que en caso de conflicto entre derechos, se privilegie a aquel que supere estas evaluaciones en el rango y medida que mejor favorezca a la persona. En consecuencia, desde esta perspectiva, el modelo constitucional ecuatoriano coincide con el modelo europeo por lo que en este ámbito también resulta aplicable.

De ese modo, los posibles conflictos entre este derecho fundamental y otros derechos, incluso de carácter económico —y dado que el artículo 11 de la Constitución establece que "todos los principios y los derechos son inalienables, irrenunciables, indivisibles, interdependientes y de igual jerarquía"— deben ser resueltos mediante la ponderación, por la cual para el caso concreto se deberá determinar una limitación razonable, proporcional y necesaria de uno de ellos frente a otro u otros, conforme a los principios de la propia Constitución. Por el cual uno de estos derechos en conflicto se verá limitado o subordinado, pero solo para el caso concreto, "salvo que haya sido el propio legislador el que mediante ley haya regulado un derecho mediante una ponderación general, pero igualmente razonable, necesaria y proporcional".[1612]

e) Necesidad de armonización. Los avances de la ciencia y la tecnología en las últimas décadas han motivado el reconocimiento paulatino del derecho a la protección de datos personales y su regulación. Desde su antecedente más inmediato en 1980, mediante la recomendación del Consejo de la Unión Europea relativa a los Flujos Transfronterizos para el Desarrollo Económico y Social, así como su desarrollo mediante la ahora derogada Directiva 95/46/CE del Parlamento Europeo, y del Consejo y del actual Reglamento (UE) 2016/679 del Parlamento Europeo, y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.[1613] Esta armonización llegó hasta los países latinoamericanos incluido Ecuador, pues en el caso de que se pretenda un intercambio natural de bienes y servicios con la Unión Europea es necesario ser declarado de nivel adecuado. De no ser el caso, se deben

[1612] A. GRIJALVA JIMÉNEZ, *Constitucionalismo en Ecuador* (Quito: Corte Constitucional para el Período de Transición, 2012), 77.
[1613] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.

implementar otros mecanismos de interacción al tenor del modelo norteamericano por el cual se necesita de normativas expresas de intercambio que, además de estar en revisión continua, no son tan dinámicas ni eficientes y tampoco no brindan garantías suficientes a los ciudadanos.

f) Marco sólido y coherente. Como se analizó en el segundo capítulo, motivación suficiente para dictar normativa a nivel de Reglamento en la Unión Europea, fue la realidad existente, por la cual, los desarrollos tecnológicos, especialmente en lo denominado la ciencia de los datos y sus diversas aplicaciones a tecnologías emergentes, que determina la necesidad de establecer un marco homogéneo y coherente de protección, que busca su universalización. De este modo, la seguridad jurídica tanto de las personas físicas, operadores económicos y autoridades públicas generen un ambiente de confianza que facilite el desarrollo de la economía digital.

El mecanismo por el cual se intenta lograr este marco sólido es una norma que equipare a los Estados miembros y a los asociados, de tal manera que los derechos y las obligaciones legales sean uniformes. Así, se pretende que, al mismo tiempo que se protege a la persona, se eliminan obstáculos a la circulación de datos personales.[1614]

El Ecuador carece de norma específica para la materia, por eso debe buscar su adopción con la finalidad de afianzar un marco sólido y coherente. Cada día se evidencia aún más la necesidad fáctica de este nivel de protección, ya que como se vio en su momento, no somos ajenos a los peligros, riesgos, abusos y transgresiones a derechos fundamentales producidos por un uso inadecuado de datos personales de ecuatorianos.

g) Flujos transfronterizos. Los flujos transfronterizos de datos en el mundo y en la Unión Europea son una realidad, producto de la globalización y del modelo económico, social y cultural de integración tanto en el ámbito público como en el privado; de los progresos tecnológicos especialmente en la recolección masiva y procesamiento de grandes volúmenes de información, incluso de aquella desestructurada (*big data*).[1615] Por esa razón, se vuelve fundamental una norma que regule el intercambio adecuado de datos que permita un flujo informacional al mismo tiempo que garantice el ejercicio de los derechos a sus ciudadanos y la protección de sus datos personales, de otras libertades individuales y derechos fundamentales.

h) Libre flujo informacional. Si bien, el modelo aplicable es el europeo, tampoco se debe desconocer aquellas circunstancias que desde el modelo americano suelen argumentarse y que se refieren a la necesidad de que existan diversos mecanismos de regulación que permitan un intercambio ágil, eficiente y práctico de los datos personales, toda vez que su dinámica permite el desarrollo de la innovación y de la economía digital. En este sentido, el citado reglamento europeo incluye un elemento nuevo no contemplado en normativas latinoamericanas, se relaciona con la determinación imperativa en el objeto de la ley, relativa a que "la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".[1616] Norma que tiene por espíritu aclarar que no se puede usar como excusa para afectar la circulación del dato a su tratamiento.

[1614] Ibíd.
[1615] Considerando (5) BOE.
[1616] Ibíd.

De lo analizado, además de confirmar que el modelo aplicable al Ecuador es el europeo, es evidente la imperiosa necesidad de una norma de protección de datos personales para Ecuador. Con la finalidad de no quedar rezagada en la región, toda vez que únicamente Bolivia, Venezuela y Panamá no cuentan con este cuerpo legal.

Como se analizó en el capítulo cuarto de este estudio, no todos los países reconocen el derecho fundamental a la protección de datos personales, sino que varios aún se aferran a la intimidad o a la privacidad en sus normas constitucionales: Bolivia, Chile, El Salvador, Guatemala, Honduras, Paraguay, República Dominicana y Cuba. Otros como Panamá y Ecuador, pese a reconocer el derecho fundamental, no han dictado norma de aplicación general que desarrolle el derecho. Varios países latinoamericanos ya cuentan con versiones legales que, aunque susceptibles de actualización, pueden generar una cultura de protección, desarrollen experiencia en el quehacer de las actividades públicas y privadas; en suma, una sociedad más consciente de los riesgos y por ende más preparada para enfrentar los posibles daños que pudieran producirse.

Es evidente que una propuesta de Ley de protección de datos personales debe contener una visión completa, integral, de alto estándar que siendo garantista de derechos fundamentales contenga mecanismos que favorezcan la innovación y el desarrollo económico del Ecuador, toda vez que se apunta en él a una transformación digital que permita promover el desarrollo económico.

En consecuencia, esta ley deberá describir en el artículo destinado al objeto aquellas temáticas a las que nos hemos referido: el establecimiento de un régimen de protección de las personas físicas en lo que respecta al tratamiento de los datos personales; la descripción de derechos y obligaciones que permitan la protección de derechos y libertades fundamentales de las personas físicas y, en particular, el derecho a la protección de los datos personales; además, una regulación relativa a la libre circulación de tales datos. En otras palabras, un contenido muy similar al señalado en el artículo 1 del RGPD,[1617] previamente analizado.

Cabe destacar que el considerando (153) del RGPD señala que "a fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio". De esta manera queda claro que el ámbito de aplicación de una normativa de protección de datos excluye las actividades periodísticas en su mayor rango de cobertura.

Ahora bien, varias de las normas latinoamericanas determinan que el objeto de la ley es la protección integral de los datos personales asentados en registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos o privados destinados a dar informes para garantizar el derecho al honor y a la intimidad de las personas, como también el acceso a la información que sobre las mismas se registre.[1618] Es decir, son normas que se refieren en realidad al ámbito de protección material, pues describen la naturaleza de los datos, los tipos de soporte y la referencia de que a través de los inadecuados tratamientos se puede afectar no solo al derecho a la protección de datos, sino a otros derechos al honor y a la

[1617] Ibíd.

[1618] Artículo 1, Congreso de la República Argentina, "Ley 25.326 de Protección de los Datos Personales", Dirección Nacional del Sistema Argentino de Información Jurídica, SAIJ., 11 de febrero de 2000, http://www.saij.gob.ar/25326-nacional-ley-proteccion-datos-personales-lns0004499-2000-10-04/123456789-0abc-defg-g99-44000scanyel.

intimidad, entre otros. En consecuencia, este contenido debe ser traslado al artículo 2 relativo al ámbito material.

De otro lado, Argentina, República Dominicana y Colombia colocan en el artículo relativo al objeto, el ámbito de inaplicación, es decir los hechos, sujetos o situaciones que son parte o se regulan por otros derechos, como por ejemplo la libertad de expresión, cuando señala que "en ningún caso se afectarán las fuentes de información periodísticas";[1619] o "En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas";[1620] o "Las bases de datos y archivos de información periodística y otros contenidos editoriales".[1621] Situación que debe ser evaluada en Ecuador debido a las experiencias fallidas de los tres proyectos presentados en la Asamblea Nacional que, entre otros criterios, fueron descalificados por atentar contra la libertad de expresión.[1622] Sin embargo, se considera que en purismo legislativo debe constar en el artículo 2 relativo al ámbito.

México establece un elemento que debe ser considerado sobre todo en el escenario latinoamericano y es la necesidad de que el objeto de la ley se haga hincapié en la promoción, fomento y difusión de una cultura de protección de datos personales.[1623]

Finalmente, el artículo 385 de la Constitución ecuatoriana establece que:

> [...] el sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:
>
> 1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.
>
> 2. Recuperar, fortalecer y potenciar los saberes ancestrales.
>
> 3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

El desarrollo o crecimiento económico es objetivo de la Constitución desde una visión integral y sustentable, por la que se exige que la actividad económica sea un medio de realización de derechos, de tal forma que se respete la libertad de contratación, la libre empresa y el uso de los datos personales con fines económicos *intra y extra* frontera; es decir:

[1619] Artículo 1, Congreso Nacional de República Dominicana, *Ley 172-13* cuyo objeto es la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes sean estos públicos o privados, 13 de diciembre de 2013, vLex, accedido 28 de enero de 2018, https://do.vlex.com/vid/personales-archivos-bancos-cnicos-informes-516279706.
[1620] Congreso de la República Argentina, *Ley 25.326 de Protección de los Datos Personales*.
[1621] *Ley protección de datos personales (Ley 1581 de 2012)* - vLex Global, 17 de octubre de 2012, https://app-vlex-com.bibliotecavirtual.udla.edu.ec/?r=true#WW/search/content_type:6/Ley+1581+de+2012+colombia/WW/vid/404685117.
[1622] "Gabriela Rivadeneira: 'En ningún momento ley restringirá datos de funcionarios públicos'", *El Comercio*.
[1623] Artículo 2, Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en posesión de sujetos obligados*, Corpus iuris en materia de protección de datos personales / INAI /RIPD, 26 de enero de 2017, http://corpusiurispdp.inai.org.mx/iberoamericano/Instrumentos/LGPDPPSO.pdf.

> [...] la Constitución ecuatoriana no concibe el desarrollo como contradictorio, sino como estructuralmente vinculado a un modelo sustentable. En tal sentido, el crecimiento económico, pese a su importancia, no es más que una de las varias dimensiones del desarrollo integral, pues este se expresa en un régimen completo que incluye dimensiones culturales, sociales y ambientales (art. 275), orientado a efectivizar el buen vivir y los derecho constitucionales... Se trata entonces de un sistema económico subordinado a y en función de la realización de los derechos de personas y colectividades (desarrollo humano), los cuales son componentes centrales del principio del buen vivir.[1624]

En tal sentido, el derecho a la protección de datos, que tiene también una dimensión económica debido a que en la sociedad red es fuente directa de riqueza. Se dice que incluso la mina de oro de la era tecnológica son los datos personales que son utilizados para direccionar negocios, empresas en el plano privado y políticas públicas, intenciones de voto, entre otros.

Es decir, coincide Ecuador con la visión europea que determina que la tecnología detrás del tratamiento de datos personales debe tener como finalidad precisamente el desarrollo social, económico, cultural que impulse la producción nacional, eleve la eficiencia y productividad, mejore la calidad de vida y contribuya a la realización del buen vivir.

La norma que se pone a consideración es la siguiente:

> **Artículo 1.- Objeto.-** El objeto de la presente Ley Orgánica es regular el ejercicio del derecho a la protección de datos personales, la autodeterminación informativa y demás derechos digitales en el tratamiento y flujo de datos personales, a través del desarrollo de principios, derechos, obligaciones y mecanismos de tutela.

2.2 Ámbito

Identificado que el modelo referente es el europeo, sin embargo por tratarse de una normativa aplicable a un país latinoamericano que tiene realidades políticas, sociales, económicas, jurídicas y culturales propias es necesario verificar que criterios que responden a nuestra idiosincrasia pueden construir un contenido aplicable al Ecuador. Para lo cual, a la luz del modelo norteamericano y sobre todo del latinoamericano, se mirarán aquellas figuras jurídicas que pueden resultar aplicables para enriquecer y responder a estas circunstancias descritas.

En este sentido, se debe coincidir con la metodología empleada en la elaboración del reglamento europeo al determinar dos ámbitos de aplicación: el material y el territorial, y dentro del primero el ámbito de inaplicación. Planteamiento de la cuestión que sin duda facilita comprensión y el futuro empleo de la norma.

Por ello se analizará a la luz del RGPD el contenido relativo al ámbito, que será cotejado con la normativa latinoamericana, las Recomendaciones de Naciones Unidas y de la Red Iberoamericana de Protección de Datos; en especial se realizará un proceso de adaptación a la normativa ecuatoriana:

[1624] GRIJALVA JIMÉNEZ, *Constitucionalismo en Ecuador*, 77.

2.2.1 Ámbito material

Respecto del ámbito material, el artículo 2 del RGPD señala que una norma sobre protección de datos personales se aplica a:

a) *Datos automatizados*. Ya sea el tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

b) *Tratamiento de datos personales por parte de instituciones y organismos comunitarios*. Esta disposición es aplicable únicamente al entorno europeo debido a que en él existen varios organismos encargados de viabilizar la integración de los países miembros.

c) *Tratamiento de datos por parte de prestadores de servicios intermediarios en comercio electrónico*. Es decir, se considera al prestador de servicios de mera transmisión como no responsable de los datos transmitidos, a menos que: "Artículo 12 [...] a) no haya originado él mismo la transmisión; b) no seleccione al destinatario de la transmisión; y c) no seleccione ni modifique los datos transmitidos. 2. Las actividades de transmisión y concesión de acceso enumeradas en el apartado 1 engloban el almacenamiento automático, provisional y transitorio de los datos transmitidos, siempre que dicho almacenamiento sirva exclusivamente para ejecutar la transmisión en la red de comunicaciones y que su duración no supere el tiempo razonablemente necesario para dicha transmisión".[1625]

Al respecto, se concluye que los elementos que se pueden tomar para elaborar nuestra propuesta de ámbito material son: la automatización parcial, total o futura y la aclaración de que a los prestadores de servicios intermediarios (mera transmisión) les es aplicable una Ley de Protección de Datos cuando cumplan con las condiciones previamente citadas.

2.2.2 Condiciones particulares de la normativa latinoamericana

Asimismo, y al tenor de las distintas normativas latinoamericanas se colige que debido a la necesidad de generar y afianzar un conocimiento y una cultura de protección de datos personales, es necesario explicitar ciertos elementos que ayuden a comprender el ámbito de aplicación material en Ecuador. Es decir, elementos como:

a) *Ámbito público y privado.* Mientras en Europa esta temática no está en discusión, en Latinoamérica se tiene varios países en los que se han legislado leyes de protección de datos personales, aplicables únicamente al ámbito público o al privado, como es el caso de Guatemala y El Salvador que hasta la presente fecha solo lo han regulado en el ámbito público. El de *Nicaragua*, que desde 1995 protege ficheros públicos, pero desde 2014, también incluye ficheros privados. El de México que dictó una norma en el año 2010

[1625] "Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) EUR-Lex - 32000L0031 - ES", text/html; charset=UNICODE-1-1-UTF-8, Diario Oficial n° L 178 de 17/07/2000 p. 0001 - 0016;, 31, accedido 8 de septiembre de 2018, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:Es:HTML.

aplicable únicamente al sector privado, y solamente en el año 2017 promulgó una norma aplicable al sector público.

De ese modo, se vuelve imperioso aclarar esta temática en la norma ecuatoriana. De los veintiún (21) países latinoamericanos analizados, se colige que es indispensable la concepción de una dimensión completa de protección. Esta norma debe regular tanto al ámbito público como al privado, pues el sistema debe ser integral, coherente y uniforme, debido a que solo de esta manera es posible el ejercicio pleno de los derechos de las personas en sociedad, de la garantía de otros derechos y libertades fundamentales, así como de la democracia misma.

La forma en la que se aborda esta redacción establece que esta norma se aplica tanto a "bases de datos personales públicas y privadas", Colombia, Perú, Uruguay. Sin embargo, con la finalidad de evitar confusiones, pues no queda claro si las bases son públicas o privadas en virtud de la naturaleza de los datos que las conforman o de los responsables de las mismas, es preferible utilizar la redacción Argentina, cuyo artículo 1, de la Ley 25.326 de 2000 de Protección de Datos Personales, señala que la presente ley tiene por objeto "la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados". En su caso, la versión de *Costa Rica*, la Ley 8968/2011 determina que la ley protege datos personales que se encuentran en bases de datos automatizadas o manuales, incluidas modalidades de uso posterior de datos, tanto de organismos públicos como privados.

Por su parte, las Recomendaciones de las Naciones Unidas sobre protección de datos personales también incluyen la referencia respecto a los archivos informatizados públicos y privados (art. 10),[1626] así como los Estándares de protección de datos personales para los Estados Iberoamericanos, sugeridos por la Red Iberoamericana de Protección de Datos, proponen en el "*ámbito de aplicación subjetivo 3.1. [...] los presentes Estándares serán aplicables a las personas físicas o jurídicas de carácter privado, autoridades y organismos públicos, que traten datos personales en el ejercicio de sus actividades o funciones*".

Por su parte, el artículo 92 de la Constitución de 2008 acerca del *habeas data* da luces sobre esta temática al señalar que mediante esta acción el titular tendrá derecho a "*conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas*".

En consecuencia, la norma ecuatoriana debe contemplar plenamente descrita que el ámbito de aplicación afecta a responsables de tratamiento de los sectores públicos o privados.

b) *No será aplicable a fuentes de información periodística*. Como se analizó previamente, debido a las experiencias fallidas de los tres proyectos presentados con anterioridad a la

[1626] Asamblea General de Naciones Unidas, "Res 45/95 Principios rectores para la reglamentación de los ficheros automatizados de datos personales", Documentos oficiales de las Naciones Unidas, 15 de diciembre de 1989, http://www.un.org/es/comun/docs/?symbol=%20A/RES/45/95&Lang=S.

Asamblea Nacional,[1627] es necesario aclarar desde un inicio que esta norma no limita la libertad de expresión ni de investigación periodística. Por ello, se adopta una combinación entre el texto constante en la normativa argentina y la colombiana que dice: "En ningún caso se podrán afectar la base de datos, archivos ni las fuentes de información periodísticas y otros contenidos editoriales".

c) *Aplicación de las directrices a archivos de datos personales mantenidos por organizaciones internacionales gubernamentales*. Las Recomendaciones de las Naciones Unidas sobre protección de datos personales señalan que:

> Las presentes directrices serán de aplicación a los archivos de datos personales que mantengan las organizaciones internacionales gubernamentales, sujetas a cualquier ajuste que sea preciso para tener en cuenta cualquier diferencia que pueda existir entre archivos para fines internos, como aquellos que conciernen a la gestión de personal, y archivos para fines externos, relativos a terceros que tengan relaciones con la organización. Cada organización debe designar a la autoridad legalmente competente para supervisar la observancia de estas directrices. Cláusula humanitaria: puede preverse específicamente una excepción a estos principios cuando la finalidad del archivo sea la protección de los derechos humanos y las libertades fundamentales de la persona afectada, o la ayuda humanitaria. Debe preverse una excepción similar en la legislación nacional para las organizaciones internacionales gubernamentales cuyo acuerdo organizativo no impida la puesta en práctica de la referida legislación nacional, así como para las organizaciones internacionales no gubernamentales a las que sea aplicable esta ley.[1628]

Ecuador, como parte de la Naciones Unidas y por expresamente solicitarlo esta recomendación, debe revisar la posibilidad de incluir esta directriz.

d) A los archivos de datos personales referidos a personas fallecidas. El RGPD en el considerando (27) señala que "el presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas". Y aunque no lo incluye dentro del articulado, sin duda es claro el precepto de dejar por fuera del ámbito de protección este tipo de datos. Por su parte, la normativa de República Dominicana señala como ámbito de inaplicación, los datos de las personas fallecidas, aunque reconoce que aquellas "personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los archivos de datos personales o tratamientos que contengan datos de este con la finalidad de notificar el fallecimiento, aportando acreditación suficiente del mismo".[1629] Otras normativas abordan la temática desde el ámbito subjetivo o de titularidad; sin embargo, esta visión resulta más clara y precisa.

e) A los tratamientos de datos referidos a personas jurídicas, ni a los archivos de datos personales que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquellas, consistentes en sus nombres y apellidos, las funciones o puestos

[1627] "Gabriela Rivadeneira: 'En ningún momento ley restringirá datos de funcionarios públicos'", *El Comercio*.
[1628] Asamblea General de Naciones Unidas, http://200.33.14.21:83/20121122060127-12869.pdf.
[1629] Congreso Nacional de República Dominicana, *Ley No. 172-13.*

desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales,[1630] la normativa de República Dominicana señala como ámbito de inaplicación esta temática que resulta muy práctica y que evita confusiones de inicio, sobre todo en aras de impedir afectaciones al comercio.

2.2.3 Ámbito de inaplicación

El RGPD determina que no será aplicable el tratamiento de datos personales que caigan en los siguientes supuestos, que serán analizados a la luz de la normativa latinoamericana, recomendaciones de Naciones Unidas, de la Red Iberoamericana de Protección de Datos Personales y de la normativa ecuatoriana.

a) *Ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión*, "como las actividades relativas a la seguridad nacional" (considerando [16], RGPD). Los supuestos descritos en la normativa europea han sido afrontados en la normativa latinoamericana desde la perspectiva de omisión del consentimiento y consecuente disposición legal que la suple. Por ejemplo, respecto de los temas relativos a defensa nacional o seguridad pública y represión de delitos, Argentina, Nicaragua, Uruguay, México y Colombia señalan que se releva de autorización del titular el tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia. La Constitución del Ecuador de 2008 señala en el artículo 393 que "el Estado garantizará la seguridad humana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos. La planificación y aplicación de estas políticas se encargará a órganos especializados en los diferentes niveles de gobierno".

   A la luz de esta norma, se considera que la normativa europea es muy amplia, por lo que es preferible que respecto de esta temática se mantenga la versión latinoamericana que determine la aplicación del régimen de protección de datos personales para los relacionados con seguridad nacional y únicamente omitir el consentimiento que en realidad está cubierto por la autorización legal.

b) *Política común de seguridad y defensa* que forma parte integrante de la política exterior y de seguridad relacionadas con la capacidad operativa basada en medios civiles y militares para recurrir en misiones fuera de la Unión, cuyo objetivo sea garantizar el mantenimiento de la paz, la prevención de conflictos y el fortalecimiento de la seguridad internacional, conforme a los principios de la Carta de las Naciones Unidas y el artículo 42 del Tratado de la Unión Europea. Este ámbito de inaplicación no es adaptable, pues su contenido es propio de los procesos de integración europeo.

c) *Efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas*.[1631] Coinciden con esta postura prevista en el RGPD, Colombia[1632] y Costa Rica[1633] que consideran a los datos domésticos como parte del

[1630] Ibíd.
[1631] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.
[1632] *Ley protección de datos personales (Ley 1581 de 2012)* - vLex Global.

ámbito de inaplicación conforme consta en los artículos 2 de cada normativa. Por su parte, Uruguay señala que no será necesario el previo consentimiento cuando se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico; es decir, se trata esta temática desde el consentimiento. En el caso de Perú, queda por fuera del ámbito de aplicación los datos creados para fines relacionados a su vida privada o familiar; no se usa el término doméstico.

Los Estándares de protección de datos personales para los Estados Iberoamericanos señalan que "*datos personales destinados actividades exclusivamente en el marco de la vida familiar o doméstica de una persona física, esto es, la utilización de datos personales en un entorno de amistad, parentesco o grupo personal cercano que no tengan como propósito una divulgación o utilización comercial*". En consecuencia, este es un elemento que debe constar en la normativa ecuatoriana.

d) Por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención. Incluidos los organismos privados que pudieran terminar relacionados, al tenor de lo señalado en el RGPD.[1634] En el caso de los países latinoamericanos, Colombia establece que no le será aplicable el régimen de protección de datos personales a las bases de datos o archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo o que contengan información de inteligencia y contrainteligencia. Según lo señalado en líneas precedentes, no estamos de acuerdo con esta postura sino con aquella que establece que le es aplicable el sistema de protección, pero que su recogida no necesita consentimiento en virtud de autorización legal.

e) Datos de población y vivienda y financieros, crediticios y comerciales. Colombia también plantea que estén fuera del ámbito de aplicación de la ley lo relativo a censos de población y vivienda (Ley 79 de 1993) y aquella sobre datos financieros, crediticios y comerciales (Ley 1266 de 2008). Ahora bien, se considera que los principios sobre protección de datos les son aplicables por lo que es mejor un régimen que regule un régimen especial en atención a la naturaleza especial de estos datos, por lo que la normativa propia de cada temática debe aplicarse de forma concurrente con la Ley de Protección de Datos.

f) Datos anónimos. Los estándares de protección de datos personales para los Estados Iberoamericanos, sugeridos por la Red Iberoamericana de Protección de Datos, proponen que también queden por fuera del ámbito de aplicación los datos anónimos, aquellos que no guardan relación con una persona física identificada o identificable. Así como aquellos sometidos a proceso de anonimización, de tal manera que el titular no pueda ser identificado o reidintificado. Al respecto, existen varios criterios que consideran que no es posible una anonimización irreversible y que siempre habrá métodos actuales o futuros que permitan reidintificar los datos; sin embargo, de ser esto posible dejarán de ser

[1633] Asamblea Legislativa de la República de Costa Rica, *Ley de Protección de la Persona frente al tratamiento de sus datos personales* 8968, 7 de julio de 2011, Sistema Costarricense de Información Jurídica, http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&param2=1&strTipM=TC&lResultado=3&strSim=simp.
[1634] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.

anonimizados y, por ende, volverán al ámbito de protección de la ley, por lo que podría ser incluido en el texto propuesto.

g) El reglamento europeo aborda esta temática en las definiciones de datos y no en el ámbito.

2.2.4 Ámbito territorial

El artículo 3 del RGPD señala el ámbito territorial de aplicación de esta norma, conforme lo siguiente:

1. *Tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea, independientemente de si el tratamiento tiene lugar en la Unión o no*. Es decir, si realiza sus actividades en cualquiera de los países miembros de la Unión Europea, sin importar que el tratamiento no se haga en dicho territorio. Este criterio es uniforme, debido a que esta normativa es vinculante con aquellos responsables o encargados de tratamiento que realicen actividades por parte de establecimientos o similares en el territorio del país. Coincide con esta postura la normativa República Dominicana, Colombia y Perú, que determina que la ley rige en todo el territorio nacional. En ese sentido consta el numeral 5.1 del ámbito de aplicación territorial de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.[1635]

   El en caso colombiano, además, se determina que "La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales".[1636]

   De conformidad con la normativa ecuatoriana, es evidente que el ámbito de aplicación es territorial.

2. *Tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión*, cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago y el control u observación del comportamiento del interesado, en la medida en que este tenga lugar en la Unión. Se usa el término *interesado* para no excluir de este sistema de protección a una persona por su nacionalidad; más bien, el criterio vinculante es la residencia.

   Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos coinciden completamente con el texto de la normativa europea. Por lo que, estos criterios debieran incorporarse en una norma ecuatoriana, tomando en cuenta criterios como el concepto de establecimiento con modalidades estables, toda vez que se intenta clarificar el ejercicio efectivo y real de actividades realizadas por el responsable o encargado del tratamiento.

[1635] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*, 20 de junio de 2017, http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf.
[1636] *Ley protección de datos personales* (Ley 1581 de 2012) - vLex Global.

Pero además, la Red Iberoamericana de Protección de Datos Personales establece los siguientes criterios a tomarse en cuenta:

a) *Derivado de la celebración de un contrato o en virtud del derecho internacional público*. La citada Red propone el siguiente texto: "5.1 Los estándares serán aplicables al tratamiento de datos personales efectuado: [...] c. Por un responsable o encargado que no esté establecido en un Estado Iberoamericano pero le resulte aplicable la legislación nacional de dicho Estado, derivado de la celebración de un contrato o en virtud del derecho internacional público".[1637]

b) *Utilice o recurra a medios, automatizados o no, situados en ese territorio*. La mencionada Red Iberoamericana propone que el siguiente texto: "5.1 Los estándares serán aplicables al tratamiento de datos personales efectuado: [...] d. Por un responsable o encargado no establecido en territorio de los Estados Iberoamericanos y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito".[1638]

c) *Grupo empresarial*. La Red Iberoamericana sugiere el siguiente texto: "5.4 Cuando el tratamiento de datos personales lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control deberá considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine efectivamente otra de las empresas del grupo".

Respecto de estas sugerencias, únicamente la ley mexicana[1639] hace análisis de estas propuestas pero no en el ámbito, sino en el capítulo sobre datos trasfronterizos.

3. *Aplicación del Derecho Internacional Público*. El RGPD se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión, sino en un lugar en que el derecho de los Estados miembros sea de aplicación en virtud del derecho internacional público, por ejemplo en el caso de "una misión diplomática u oficina consular de un Estado miembro" (considerando [25], RGPD).[1640]

Respecto de esta temática, Colombia determina que "La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales".[1641]

De conformidad con la normativa ecuatoriana, este ámbito de aplicación es procedente en virtud de la aplicación de tratados internacionales.

[1637] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1638] Ibíd.
[1639] Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en posesión de sujetos obligados*.
[1640] Considerando 23, BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.
[1641] *Ley protección de datos personales (Ley 1581 de 2012)* - vLex Global.

Luego del análisis presentado, se pone en consideración el siguiente texto relativo al ámbito de aplicación de esta norma:

> ***Artículo 3.- Ámbito de aplicación material***.- *La presente Ley Orgánica se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, ya sean totalmente automatizados, parcialmente automatizados o no automatizados y a toda modalidad de uso posterior, por parte de responsables o encargados del tratamiento de datos personales.*
>
> ***Artículo 4.- Ámbito de aplicación territorial***.- *Sin perjuicio de la normativa establecida en los convenios y tratados internacionales ratificados por el Estado ecuatoriano que versen sobre esta materia se aplicará la presente Ley Orgánica cuando:*
>
> *El tratamiento de datos personales se realice en cualquier parte del territorio nacional;*
>
> *El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional;*
>
> *El responsable o encargado del tratamiento de datos personales que no se encuentre domiciliado en el Ecuador y que oferte bienes o servicios a personas localizadas en el territorio nacional, independientemente de si se requiere su pago o no;*
>
> *El responsable o encargado del tratamiento de datos personales que no se encuentre domiciliado en el Ecuador y que realice actividades relativas a la recogida de datos personales de personas localizadas en el territorio nacional; y,*
>
> *Al responsable o encargado del tratamiento de datos personales no domiciliado en el territorio nacional le resulte aplicable la legislación nacional en virtud de la celebración de un contrato o del derecho internacional público.*
>
> ***Artículo 5.- Ámbito de exclusión***.- *El régimen de protección de datos personales que se establece en la presente Ley Orgánica no será de aplicación para:*
>
> *Personas naturales que utilicen estos datos en la realización de actividades familiares o domésticas;*
>
> *Personas fallecidas, sin perjuicio de lo establecido en el artículo 38 de la presente Ley Orgánica;*
>
> *Datos anónimos;*
>
> *Fuentes de información y otros contenidos editoriales de naturaleza periodística;*
>
> *Datos personales cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía en materia de gestión de riesgos y desastres naturales; y, seguridad nacional y defensa del Estado;*

Cuando se trate de datos personales relativos a la salud, únicamente cuando estos tengan por finalidad evitar poner en riesgo a la población; es decir, para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados;

Datos o bases de datos establecidos para la prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales; y,

Datos que identifican o hacen identificable a personas jurídicas.

Son accesibles al público y susceptibles de tratamiento los datos personales de contacto de comerciantes; representantes y socios de personas jurídicas; así como los de servidores públicos siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo.

El histórico y vigente de la declaración patrimonial y de la remuneración para el caso de servidores públicos, por la naturaleza de su cargo, se considerará accesible al público y susceptible de tratamiento.

2.3 Naturaleza del dato

Respecto de la naturaleza del dato, en el caso de una propuesta de normativa para Ecuador, se debe llevar el nivel de análisis a los conceptos más básicos debido a las confusiones traídas, sobre todo, desde la jurisprudencia ecuatoriana, que señala que solo es posible la protección de los datos que tienen carga informativa y no todo tipo de dato.[1642]

a) *Dato o información* al respecto, Davara sostiene que:

> [...] dato es el antecedente o noticia que sirve de punto de partida para la investigación de la verdad [...] son las noticias de su origen, sin haber sido sometidas a ningún tipo de tratamiento ni adecuación. [...] La información será el resultado orientado y adecuado a un fin determinado. [...] Todos estos datos, organizados mediante los sistemas automatizados de almacenamiento y recuperación de la información, deben estar protegidos contra el acceso —malintencionado o no— de quienes no estén autorizados para ello. La protección se realiza, consiguientemente, sobre el dato, para que éste no pueda ser tratado o elaborado, y convertido en información, nada más que para aquellos fines y por aquellas personas autorizadas a ello.[1643]

De lo descrito, tanto el dato como la información son relevantes debido a que por medio de metodologías de organización un dato e incluso un metadato sometido a un tratamiento puede llegar a revelar perfiles completos de la personalidad. Entonces, la jurisprudencia del país debe ser aclarada en la norma ecuatoriana estableciendo como base del sistema de protección a los datos personales. No debe usarse término "información" desde la acepción de que es el dato con carga informativa, ya que esta

[1642] Corte Constitucional del Ecuador, "Sentencia No. 001-2014-PJO-CC".
[1643] M. DAVARA RODRÍGUEZ, *Manual de derecho informático* (Cizur Menor: Thomson Aranzadi, 2015), 53.

interpretación pondría en riesgo a los titulares. Si se usa el término información, se lo debe hacer como sinónimo de "dato", pues solo de esta forma se garantiza una protección integral.

En Latinoamérica, tanto aquellos países que basan su sistema de protección en la intimidad (Brasil, Paraguay, Venezuela, Chile), como los que lo hacen desde el derecho a la protección de datos personales, usan información como sinónimo de datos (Guatemala, Nicaragua, Colombia, Perú, Argentina, México, Uruguay, Costa Rica, Panamá y República Dominicana).

b) *Cualquier tipo de dato, no solo el dato íntimo*. Mediante la autodeterminación informativa las personas tienen la libertad de decidir sobre sus datos, cualquiera sea su naturaleza; es decir, no solo aquellos referidos al ámbito de su intimidad o privacidad, sino todos los datos que aparentemente inocuos pueden otorgar perfiles de personalidad, y que pueden ser usados para violentar otros derechos fundamentales distintos a la intimidad. En efecto, "la protección de datos de carácter personal no se reduce solo a los datos más íntimos de la persona sino a cualquier tipo de dato personal cuyo conocimiento o empleo por terceros pueda afectar a los derechos del que los proporciona, y por consiguiente afecta también a los datos personales públicos, que por el hecho de ser accesibles al conocimiento de terceros, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. Por tanto, los datos amparados son aquellos que permitan identificar a la persona, confeccionando su perfil ideológico, racial, sexual, económico, o de cualquier otra índole";[1644] es decir, se protegen los datos de carácter personal, anotándose que no se protegen los datos en sí mismos, sino a los titulares de esos datos.

La jurisprudencia ecuatoriana señala que el *habeas data* resguarda derechos como el honor, el buen nombre y la intimidad personal y familiar y también la protección de datos personales. De modo que esta acción constitucional protege no solo el dato íntimo, sino todo tipo de datos personales.

A fin de evitar confusiones y sobrellevar la disquisición de si se deben proteger los datos irrelevantes, o inocuos países como Nicaragua, Perú, Uruguay, Costa Rica utilizan la expresión general *todo tipo de dato*.

c) *Dato personal*. Como se analizó en el capítulo segundo, el RGPD, artículo 4, acerca de las definiciones, se entiende como datos personales a toda información sobre una persona física identificada o identificable. Este criterio se repite desde la Directiva 95/46, 24 de octubre, del Parlamento Europeo y del Consejo.

En Latinoamérica, independientemente de si el enfoque de protección es la intimidad o la protección de datos personales, es coincidente que para este sistema de protección reforzado es indispensable que esté asociado o vinculado, concerniente, relativo o sobre la persona. No obstante, existe un grupo de países, entre los que se incluye Ecuador, que al describir las acciones constitucionales de *habeas data*, además de

[1644] CONDE ORTIZ, *La protección de datos personales*, 66.

señalar que se trata de datos personales, hacen alusión a que estos son datos sobre sí mismos o de sus bienes (Paraguay, Venezuela). Dicha afirmación, lejos de aclarar al derecho lo vuelve confuso, por lo que se recomienda no incluir esta mención. Como esta acotación es propia del *habeas data* no afecta al derecho en sí mismo, y es mediante la normativa de protección de datos que se establece un concepto general que permite incluir estos y otros contextos dentro de él, pues son datos personales los que reflejan los bienes de un titular, por ejemplo.

La dirección de correo electrónico es dato personal, tanto si la dirección está formada por el nombre del titular como si está formada por caracteres que no permiten la personalización del e-mail. En el primer caso, porque la dirección de correo electrónico contiene en sí mismo un dato personal. En el segundo caso, aun cuando no se pueda obtener una identificación inicial de a quién pertenece el correo con la simple lectura de la dirección de correo electrónico, pues esta aparece referenciada a un dominio concreto que es un mecanismo de consulta del servidor que no refleja un esfuerzo desproporcionado por parte de quien procede a la identificación.[1645]

Lo mismo ocurre con los "mensajes cortos remitidos por teléfono móvil, que se almacenan junto con el número del llamante, constituyen en sí mismo datos personales, pues a través del número telefónico se puede llegar a conocer al destinatario del mensaje".[1646]

El cliente ingresa y navega en la página web y activa los faros de programación en HTML o XML, mediante *clics* deja un rastro y su información se graba en tarjetas de perfil y visita,[1647] permitiendo que los datos le sean atribuibles y que sean sometidos a un tratamiento.[1648] De este modo, se puede definir, del cliente, el perfil económico, social, sus comportamientos de compra, su estado de ciclo de vida, etc.

d) *Persona identificable*. Como se analizó en el capítulo segundo, el RGPD en artículo 4, acerca de las definiciones afirma que se "considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona". Este texto se diferencia de la Directiva 95/46, porque añade la identidad genética como uno de los ejemplos de identificador. Además, el RGPD establece que un identificador no solo es un número, sino cualquier elemento como los señalados en la lista de ejemplos citados, incluidos "los identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por

[1645] AEPD 00377/2005, 13 de junio.
[1646] Comité Consultivo de la AEPD, "Conclusiones y recomendaciones efectuadas en la Inspección Sectorial relativa a Concursos Juegos y Sorteos de Televisión", *La protección de datos de Carácter Personal en España: Análisis y valoración*, 145.
[1647] Pequeños ficheros electrónicos.
[1648] El artículo 3 de la LOPD dice: "Definiciones: A los efectos de la presente Ley Orgánica se entenderá por: [...] c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

radiofrecuencia" (considerando [30], RGPD). Pero el citado reglamento señala que "el identificador único, los identificadores en línea y otros datos recibidos por los servidores, pueden ser utilizados para elaborar perfiles de las personas físicas e identificarlas".

Se usan los términos *identificados* o *identificables* en Guatemala, Brasil, México, Bolivia, Costa Rica, Chile y República Dominicana, mientras la frase que *la identifica* o *la hace identificable* se utiliza en Nicaragua y Perú, y *determinadas* o *determinable* en Uruguay y Argentina. Aunque la terminología es distinta su comprensión es la misma, no solo se protege el dato que identifica por si solo a una persona, sino aquel dato que tratado puede llegar a identificarle, porque al proteger el dato se protege a la persona.

Respecto de la condición de identificable, Perú realiza una precisión adicional: establece que la identificación debe realizarse a través de medios que pueden ser razonablemente utilizados. Sobre razonabilidad en el uso de medios para identificar a una persona, el RGPD señala que deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Estos medios serán razonables valorando factores objetivos, como los costes y tiempo necesario para realizar la identificación, "teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos".

Además, se debe dejar la constancia en la norma el avance reflejado en el RGPD por el cual:

> [...] si los datos personales tratados por un responsable no le permiten identificar a una persona física, el responsable no debe estar obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir cualquier disposición del presente Reglamento. No obstante, el responsable del tratamiento no debe negarse a recibir información adicional facilitada por el interesado a fin de respaldarle en el ejercicio de sus derechos. La identificación debe incluir la identificación digital de un interesado, por ejemplo mediante un mecanismo de autenticación, como las mismas credenciales, empleadas por el interesado para abrir una sesión en el servicio en línea ofrecido por el responsable.

En conclusión, son datos identificativos aquellos que permiten una atribución directa como nombres, dirección, teléfono, DNI; pero también aquellos que "se pueden sumar a los identificativos para someterlos a tratamiento [...] datos de características personales, datos de circunstancias sociales, datos académicos y profesionales, datos de detalles de empleo, datos de información comercial, datos económicos-financieros, datos de transacciones y datos especialmente protegidos".[1649]

En cambio, son datos identificables aquellos para los cuales no es "imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados y para determinar si una persona es identificable, hay que considerar el conjunto de los medios que

[1649] D. SANTOS GARCÍA, *Nociones generales de la Ley Orgánica de Protección de Datos* (Madrid: Editorial Tecnos, 2005), 42.

puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona.[1650]

En consecuencia, no importa si los datos parecieran "*a priori* irrelevantes, pueden servir para una finalidad diferente y, por lo tanto, proporcionan claves insospechadas sobre la persona". Le teoría del mosaico pone de relieve como datos aparentemente inocuos pueden aportar una información preciosa a la hora de elaborar un determinado perfil personal. De modo que todos aquellos datos referentes a la persona merecen la protección que otorga la ley.[1651] Como se ve, la intencionalidad de la norma es proteger a toda costa al titular del dato que lo identifique o que permita identificarlo de manera directa o indirecta.

e) *Tipo de soporte que contiene el dato personal*. La legislación latinoamericana hace énfasis en mencionar que se protege todo tipo de soporte en el que conste el dato personal, sea físico o virtual o electrónico, tal ocurre en las legislaciones de Nicaragua, Colombia, Argentina y República Dominicana. México también incluye la aseveración de que se protege todas las formas posibles de soporte incluidos lo escrito, impreso, sonoro, visual, electrónico, informático u holográfico. Bolivia, por su parte, menciona medio físico o magnético; Honduras, el término convencional; Perú: digital, óptico; y Panamá, químico, físico o biológico.

Otros países no hacen mención al tipo de soporte; razón por la cual se entiende incluida cualquier forma (física, virtual o la que pudiera crearse), como es el caso de Guatemala, Paraguay, El Salvador o Uruguay. En la misma postura se encuentran los Estándares para los Estados Iberoamericanos y el RGPD, que no mencionan ningún tipo de soporte. Se coincide con esta postura, ya que debido a los avances tecnológicos es preferible establecer el régimen de protección por la simple condición de ser dato personal independiente del soporte en el que se encuentre, y con ello no dejar por fuera futuras tecnologías que se llegaren a desarrollar. En lugar de utilizar como parte de la definición el tipo de soporte, se prefiere usar el término "tratamiento", que a continuación se analiza.

f) *Tratamiento*. Conforme se analizó oportunamente, en el artículo 4 del RGPD, se define como tratamiento a "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción". Este concepto añade la referencia a conjunto de datos personales, precisión que debe ser tomada en cuenta en la normativa propuesta.

[1650] SAN recurso 948/2000, 8 de marzo de 2002.
[1651] M. FERNÁNDEZ ESTEBAN, *Nuevas Tecnologías, Internet y Derechos Fundamentales* (Madrid: Mc Graw Hill, 1998), 129.

Los Estándares Iberoamericanos, en la referencia 2, literal i), añaden la frase "posesión, aprovechamiento y en general cualquier uso o disposición de datos personales", la cual podría ser usada.

Las normativas de Argentina, Colombia, Costa Rica México, República Dominicana, Perú y Uruguay mencionan, entre las definiciones aplicables a sus respectivas leyes, el término "tratamiento" con una definición muy similar a la revisada previamente; solo se añaden sinónimos o criterios similares como el de procesamiento.

g) *Limitación del tratamiento*. Únicamente el RGPD señala la definición de limitación del tratamiento, en el artículo 4, numeral 3, por el cual establece "el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro".

La única referencia a limitación del tratamiento que consta en la normativa latinoamericana la tiene la Ley de Protección de Datos peruana que señala en el artículo 13, titulado alcance sobre el tratamiento de datos personales, específicamente el literal 13.2: "Las limitaciones al ejercicio del derecho fundamental a la protección de datos personales solo pueden ser establecidas por ley, respetando su contenido esencial y estar justificadas en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos". Si bien, el texto es valioso, hace referencia no a limitaciones técnicas, como hace el RGPD, sino a limitaciones al ejercicio del derecho por lo que, aun llevan nombres similares, no se refieren a lo mismo.

Es necesario incluir en la normativa ecuatoriana, tanto la referencia a la limitación del tratamiento desde la perspectiva técnica —esto es desde la necesidad de establecer el marcado de los datos—, como a la necesidad de ley y razón justificada para la limitación al derecho fundamental.

h) *Elaboración de perfiles*. El artículo 4 del RGPD señala un concepto de elaboración de perfiles, por el cual se establece que se entenderá como toda forma de tratamiento automatizado que consiste en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

En Latinoamérica no existe normativa que establezca un concepto de elaboración de perfiles, sino más bien autorizaciones, condiciones para su uso. Es el caso de la legislación de Argentina que establece prohibiciones como la señalada en el artículo 20.1., de la Ley 25.326:[1652] las decisiones judiciales o los actos administrativos que impliquen valoración de conductas humanas, no podrán tener como único fundamento el resultado de un tratamiento que suministre un perfil o personalidad del interesado; en caso de que esto se haya producido, dichas actuaciones judiciales o administrativas se consideran absolutamente nulas. También autoriza la realización de perfiles para la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, con fines promocionales, comerciales o publicitarios; o que permitan establecer hábitos de consumo cuando estos figuren en documentos

[1652] Congreso de la República Argentina, *Ley 25.326 de Protección de los Datos Personales*.

accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento, de conformidad con el artículo 27, numeral 1 de la citada ley.

Uruguay y República Dominicana establecen una norma muy similar a la Argentina respecto de la autorización con fines de publicidad, añadiendo únicamente lo relativo al derecho del titular de los datos a ejercer el derecho de acceso sin cargo alguno, y solicitar el retiro o bloqueo de sus datos de los bancos de datos, conforme el artículo 21 de la Ley 18.331[1653] y artículo 71 de la Ley 172-13,[1654] respectivamente.

Este tema ha cobrado fuerza debido a los avances en analítica de datos que facilitan cada vez más completos y precisos perfiles de personalidad, cuyos resultados se están usando con finalidades distintas a las autorizadas por la ley y que pudieran, incluso, convertirse en mecanismo para manipulación de voluntades y, por ende, significar una transgresión a las libertades individuales.

i) *Seudonimización*. Este concepto se lo trata por primera vez en el artículo 4.5 del RGPD, determinando que consiste en el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física, identificada o identificable.

En Latinoamérica no existe mención sobre seudonimización; por el contrario, se habla de anonimización o de disociación de datos, al tenor de los siguientes temas:

a) *Definición de anonimización o disociación*. En Argentina, el artículo 2 de la de la Ley 25.326[1655] define a la disociación de datos como todo tratamiento de datos personales, de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

México, Uruguay Nicaragua, Perú y República Dominicana coinciden con el concepto sobre disociación constante en la normativa argentina. Perú añade que el procedimiento es reversible, y República Dominicana la frase: "mediante el uso de técnicas de codificación, de modo que no permita identificar a la persona física ante terceros".

b) *Cesión de datos anonimizados*. Asimismo, en Argentina la Ley 25.326[1656] establece que solo pueden cederse datos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario, a menos que se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables (art. 11, num. 1).

[1653] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, *Ley 18.331, de Protección de Datos Personales y Acción de Habeas Data*, 11 de agosto de 2008, D.O., 18 de agosto de 008 - 27549, 2008, https://parlamento.gub.uy/documentosyleyes/leyes?Ly_Nro=18331&Ly_fechaDePromulgacion%5Bmin%5D%5Bdate%5D=&Ly_fechaDePromulgacion%5Bmax%5D%5Bdate%5D=&Ltemas=&tipoBusqueda=T&Searchtext=.

[1654] Congreso Nacional de República Dominicana, *Ley 172-13*.

[1655] Congreso de la República Argentina, *Ley 25.326 de Protección de los Datos Personales*.

[1656] Ibíd.

c) *Disociación para encuestas de opinión, mediciones y estadísticas*. Se añade en el artículo 28, numeral 1 de la Ley 25.326[1657] que las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida en que los datos recogidos no puedan atribuirse a una persona determinada o determinable. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se utilizará una técnica de disociación, con el fin de que no permita identificar a persona alguna.

d) *Excepción de consentimiento cuando se anonimiza*. La norma argentina señala en el artículo 28, numeral 4 de la Ley 25.326[1658] que entre las obligaciones del responsable y el encargado están las de no utilizar los datos personales objeto de tratamiento para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación. En igual sentido, la norma mexicana de 2010 sobre responsables particulares en el artículo 10, III[1659] y en la de 2017 sobre sujetos obligados en el artículo 22.[1660] República Dominicana señala que también existen excepciones al consentimiento cuando se traten de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve el secreto de la identidad de los titulares de los datos mediante mecanismos de disociación adecuados o se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables (art. 27, nums. 8 y 9, Ley 172-13).[1661]

Conforme lo señalado, la referencia en la normativa ecuatoriana debe ser tanto del concepto anonimización como el de seudonimización, y la adaptación a las diferentes situaciones en las que es indispensable su aplicación.

j) *Fichero o base de datos*. El término "fichero" no es comúnmente usado en Latinoamérica, únicamente Costa Rica, Nicaragua y República Dominicana lo utilizan como sinónimo de base de datos; el resto de países latinoamericanos opta por utilizar la frase "base de datos". Aunque su significado es muy similar, el RGPD lo concibe como un "conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica" (art. 4).

Para determinar el concepto de base de datos se analizarán los siguientes criterios:

i. *Conjunto organizado de datos personales*. Colombia, en el artículo 3, literal b) de la Ley 1581[1662] determina que es el conjunto organizado de datos personales que sea objeto de tratamiento, sin entrar en más

[1657] Ibíd.
[1658] Ibíd.
[1659] Congreso General de los Estados Unidos Mexicanos, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, 7 de mayo de 2010, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.
[1660] Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en posesión de sujetos obligados*.
[1661] Congreso Nacional de República Dominicana, *Ley 172-13*.
[1662] *Ley protección de datos personales (Ley 1581 de 2012)* - vLex Global.

especificaciones. Todos los otros países latinoamericanos, incluso el RGPD, utilizan el criterio de "conjunto organizado de datos personales", siendo el más uniforme de la normativa. Incluso México en la normativa que regula particulares señala que por bases de datos se entiende al conjunto ordenado de datos personales referentes a una persona identificada o identificable (art. 3, II).[1663]

ii. *Archivo, fichero, registro, base o banco de datos*. Costa Rica, a diferencia del RGPD, incluye en el concepto a "cualquier archivo, fichero, registro" (art. 3, Ley 8968).[1664] Nicaragua habla también de "bases o bancos de datos públicos y privados" (art. 3, lit. i), Ley 787).[1665] Argentina menciona en el concepto tanto de "archivo, registro, base o banco de datos indistintamente, pues designan un conjunto organizado de datos personales" (art. 2, Ley 25326).[1666] República Dominicana determina como concepto el de archivo, registro, ficheros, base o banco de dato (art. 6, nums. 2 y 25, Ley 172-13).[1667] Argentina menciona indistintamente los términos citados pues en suma designan al conjunto organizado de datos personales (art. 2, Ley 25326).[1668]

iii. *Objeto de tratamiento o procesamiento, automatizado o manuales*. Costa Rica determina que una base de datos debe ser objeto de tratamiento o procesamiento, automatizado o manual (art. 3, Ley 8968).[1669] Mientras Nicaragua únicamente menciona que "contienen de manera organizada los datos personales, automatizados o no" (art. 3, lit. i), Ley 787).[1670] Argentina y Uruguay añaden que el tratamiento o procesamiento, puede ser electrónico o no (art. 2, Ley 25326[1671] y art. 4, lite. a), Ley 18.331,[1672] respectivamente). En el mismo sentido, la normativa de República Dominicana en el artículo 6, numerales 2 y 25 de la Ley 172-13.[1673]

iv. *Cualquiera que sea la modalidad de su elaboración, organización o acceso*. Costa Rica menciona un criterio similar al expuesto en el RGPD,

---

[1663] Congreso General de los Estados Unidos Mexicanos, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*.
[1664] Asamblea Legislativa de la República de Costa Rica, *Ley de Protección de la Persona frente al tratamiento de sus datos personales*, 8968, 7 de julio de 2011.
[1665] *Ley 787, Ley de Protección de Datos Personales de Nicaragua*, 29 de marzo de 2012 - vLex Global, 29 de marzo de 2012, https://app-vlex-com.bibliotecavirtual.udla.edu.ec/?r=true#WW/search/content_type:6/nicaragua+Ley+de+Protecci%C3%B3n+de+Datos+Personales%2C+Ley+No.+787%2C+aprobada+el+21+de+Marzo+del+2012%2C+publicada+en+la+Gaceta+No.+61+del+29+de+Marzo+del+2012/p2/WW/vid/645251929.
[1666] Congreso de la República Argentina, *Ley 25.326 de Protección de los Datos Personales.*
[1667] Congreso Nacional de República Dominicana, *Ley 172-13*.
[1668] Congreso de la República Argentina, *Ley 25.326 de Protección de los Datos Personales*.
[1669] Asamblea Legislativa de la República de Costa Rica, *Ley de Protección de la Persona frente al tratamiento de sus datos personales*, 8968, 7 de julio de 2011.
[1670] *Ley 787, Ley de Protección de Datos Personales de Nicaragua*, 29 de marzo de 2012 - vLex Global.
[1671] Congreso de la República Argentina, *Ley 25.326 de Protección de los Datos Personales*.
[1672] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, *Ley 18.331, de Protección de Datos Personales y Acción de Habeas Data*, 11 de agosto de 2008, D.O. 18 ago/008 - 27549.
[1673] Congreso Nacional de República Dominicana, *Ley 172-13*.

pues establece que las bases de datos lo son tales cualquiera sea la modalidad de su elaboración, organización o acceso (art. 3, Ley 8968).[1674] Argentina y Uruguay determinan que es una base de datos cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso (art. 2, Ley 25326[1675] y art. 4, lit. a), Ley 18.331,[1676] respectivamente). Y en la normativa que regula a sujetos obligados públicos determina que son el conjunto ordenado de datos personales referentes a una persona física, identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización (art. 3 III). República Dominica en el artículo 6, numerales 2 y 25 de la Ley 172-13[1677] establece que es un conjunto organizado de datos personales cualesquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso. Perú habla además de creación y formación en el artículo 2, numeral 1 de la Ley 29733.[1678]

v. *Independiente del soporte*. Perú, por su parte, señala en el artículo 2, numeral 1 de la Ley 29733[1679] que se entenderá por banco de datos personales al conjunto organizado de datos personales, automatizado o no, "independiente del soporte, sea este físico, magnético, digital, óptico y otras que se creen".

vi. *Públicos o privados*. Nicaragua añade en este concepto la característica de que estos bancos de datos pueden ser públicos o privados (art. 3, lite. i), Ley 787).[1680] República Dominicana[1681] determina que se "Incluye también el conjunto de informaciones que proporcionan directamente los aportantes de datos, así como otras informaciones de carácter y dominio público, ya sea por su procedencia o por su naturaleza" (art. 6, num. 25, Ley 172-13).

Luego de las precisiones señaladas, es indispensable que el concepto de base de datos incluya todas las posibles variables analizadas, debido a que en Ecuador es necesario generar bases para homologar criterios; por eso no sería aconsejable optar por textos abiertos como el del RGPD, con la acotación de que las enumeraciones deben ser ejemplificativas y que, por ende, es necesario incluir frases como y cualesquiera otras que se llegaren a desarrollar, entre otras, etc. para aclarar que las listas no son taxativas.

[1674] Asamblea Legislativa de la República de Costa Rica, *Ley de Protección de la Persona frente al tratamiento de sus datos personales*, 8968, 7 de julio de 2011.
[1675] Congreso de la República Argentina, *Ley 25.326 de Protección de los Datos Personales*.
[1676] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, *Ley 18.331, de Protección de Datos Personales y Acción de Habeas Data*, 11 de agosto de 2008, D.O. 18 ago/008 - 27549.
[1677] Congreso Nacional de República Dominicana, *Ley 172-13*.
[1678] Congreso de la República del Perú, *Ley 29733*, de Protección de Datos Personales, Archivo Digital de la Legislación del Perú, accedido 5 de junio de 2017, http://www.leyes.congreso.gob.pe/LeyNume_1p.aspx?xEstado=2&xTipoNorma=0&xTipoBusqueda=4&xFechaI=&xFechaF=&xTexto=&xOrden=0&xNormaI=29733&xNormaF=29733.
[1679] Congreso de la República del Perú.
[1680] *Ley 787, Ley de Protección de Datos Personales de Nicaragua*, 29 de marzo de 2012 - vLex Global.
[1681] Congreso Nacional de República Dominicana, *Ley 172-13*.

k) *Datos genéticos*.[1682] El RGPD señala el concepto de datos genéticos, entendidos como aquellos relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona (art. 4, num. 13).

El artículo 3 de la Ley 8968[1683] de Costa Rica; el artículo 3. VI de la Ley de responsables particulares de México,[1684] y el artículo 3. X de la Ley de Sujetos Obligados, también de México,[1685] incluyen en la lista de datos sensibles a la información genética. En la normativa latinoamericana, únicamente Costa Rica menciona datos biomédicos como sensibles.

l) *Datos biométricos*. El RGPD determina que se entenderá por datos biométricos aquellos que obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos (art. 4).

Solo Colombia en el artículo 5 de la Ley 1581 y Perú en el artículo 2, numeral 5 de la Ley 29733[1686] incluyen al dato biométrico en la lista de datos sensibles.

Mientras que el artículo 60 de la Ley 172-13[1687] de República Dominicana determina que:

> [...] las Sociedades de Información Crediticia (SIC) deberán utilizar técnicas de identificación biométricas que dificulten o imposibiliten la usurpación o el robo de las identidades de las personas físicas al momento de contratar bienes y servicios ante los organismos públicos, las empresas públicas y las empresas privadas, o cualquier ente económico que utilicen los servicios de información de las Sociedades de Información Crediticia (SIC). A este respecto, las Sociedades de Información Crediticia (SIC) y los aportantes de datos deberán incluir en los reportes que emiten y en las informaciones que aportan, respectivamente, la foto actualizada o disponible del consumidor o del titular de los datos, de tal modo que el usuario de los reportes provenientes de una Sociedad de Información Crediticia (SIC) debe validar y autenticar la identidad de la persona física comparando el rostro del solicitante del bien o servicio con la imagen en el reporte de la Sociedad de Información Crediticia (SIC).

Es decir, establece un uso específico para los datos biométricos como mecanismo de prevención para usurpación o robo de identidades.

[1682] J. APARICIO SALOM, *Estudio sobre la protección de datos* (Cizur Menor, Navarra: Aranzadi, 2013), 126.
[1683] Asamblea Legislativa de la República de Costa Rica, *Ley de Protección de la Persona frente al tratamiento de sus datos personales*, 8968, 7 de julio de 2011.
[1684] Congreso General de los Estados Unidos Mexicanos, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*.
[1685] Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en posesión de sujetos obligados*.
[1686] Congreso de la República del Perú, *Ley 29733*, de Protección de Datos Personales, 3 de julio de 2011.
[1687] Congreso Nacional de República Dominicana, *Ley 172-13*.

La normativa ecuatoriana debe incluir en sus datos sensibles a los datos biométricos. Respecto de su uso por parte de sociedades de información crediticia, es importante realizar una revisión de la realidad económica ecuatoriana para verificar su implementación.

m) *Tratamiento de categorías especiales de datos personales:* Tanto el RGPD como una parte de la normativa latinoamericana establecen un régimen mayor de protección para aquellos datos considerados especiales. Los primeros que entran en esta categoría son los denominados datos sensibles, cuyo contenido y específico sistema de protección será analizado a continuación:

1. *Datos sensibles*. Los países latinoamericanos que clasifican a los datos en sensibles son Guatemala, Nicaragua, Colombia, Paraguay, Perú, Argentina, Uruguay, República Dominicana, El Salvador, Chile, México, Costa Rica y Ecuador. Los países que no mencionan la categoría de datos sensibles son Brasil, Venezuela, Bolivia, Honduras y Panamá.

   Se entienden por datos personales sensibles aquellos que revelen el origen racial o étnico, a las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. Se añaden los datos genéticos y biométricos que fueron analizados previamente, conforme señala el RGPD y el Estándar Iberoamericano de Protección de Datos Personales.

   Otros países latinoamericanos establecen como datos sensibles también la pertenencia a sindicatos, a organizaciones sociales, o de derechos humanos (Colombia); convicciones religiosas, filosóficas o morales, relativo a su salud, físicos o psíquicos (Chile), presente o futura (México), vida sexual, los datos biométricos (Perú), información biomédica o genética (Costa Rica), antecedentes penales o faltas administrativas, económicos financieros; así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación (Guatemala, Nicaragua).

   El RGPD considera datos sensibles a una categoría especial de datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. O incluso pueden dar origen a discriminación o conlleve un riego grave, conforme los Estándares Iberoamericanos de Protección de Datos Personales. En virtud de estas consideraciones, su

régimen de protección es reforzado. Por ejemplo, ninguna persona puede ser obligada a proporcionar datos sensibles (art. 17, Ley 787-2012).[1688]

Su tratamiento está prohibido (art. 9, num. 1, RGPD), a menos que se cumplan ciertas condiciones:

i. *Solo pueden ser recolectados y tratados por razones de interés general debidamente señalados en la ley*. Artículo 7 de la Ley 25.326 de Argentina;[1689] artículo 6 de la Ley 1581 de Colombia;[1690] artículo 8 de la Ley 787-2012 de Nicaragua;[1691] artículo 13, numeral 6 de la Ley 29733 del Perú;[1692] artículo 18 de la Ley 18331 del Uruguay.[1693] El Estándar Iberoamericano de Protección de Datos Personales señala que no podrá tratarse datos personales sensibles, salvo se dé cumplimiento a un mandato legal.

ii. *Consentimiento explícito del titular de datos*. El artículo 9, literal a) del RGPD requiere consentimiento explícito del titular de datos. Por su parte, el Estándar Iberoamericano de Protección de Datos Personales señala que el consentimiento debe ser expreso y por escrito.

iii. *Sean necesarios para el ejercicio y cumplimiento de atribuciones y obligaciones previstas en la norma*. Al tenor de lo señalado en el artículo 9 de los Estándares Iberoamericanos. Por su parte, la normativa de Uruguay en el artículo 18 de la Ley 18331 señala que se pueden recolectar datos sensibles cuando el organismo solicitante tenga mandato legal para hacerlo.

iv. *Sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros*. Al tenor de lo señalado en el artículo 9 de los Estándares Iberoamericanos.

v. *Organismos sin fin de lucro*. El RGPD establece que están facultados al tratamiento de datos sensibles, en el ámbito de actividades legítimas y con debidas garantías, las fundaciones, asociaciones o cualquier otro organismo sin ánimo de lucro (art. 9, lit. d), RGPD).

[1688] *Ley 787, Ley de Protección de Datos Personales de Nicaragua*, 29 de marzo de 2012 - vLex Global.
[1689] Congreso de la República Argentina, *Ley 25.326 de Protección de los Datos Personales*.
[1690] *Ley protección de datos personales (Ley 1581 de 2012)* - vLex Global.
[1691] *Ley 787, Ley de Protección de Datos Personales de Nicaragua*, 29 de marzo de 2012 - vLex Global.
[1692] Congreso de la República del Perú, *Ley 29733, de Protección de Datos Personales*.
[1693] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, *Ley 18.331, de Protección de Datos Personales y Acción de Habeas Data*, 11 de agosto de 2008, D.O. 18 ago/008 - 27549.

vi. *Defensa en juicio o ejercicio de la función judicial*. Es posible el tratamiento de datos sensibles para el ejercicio o la defensa en tribunales (art. 9, lit. f), RGPD).

2. Otro tipo de datos considerados especiales

i. *Derechos laborales y de seguridad y protección social*. Otro tipo de dato que se considera especial, según el RGPD, es aquel necesario para el "cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social". No existe referencia equivalente en la normativa latinoamericana.

ii. *Intereses vitales propios o de otros*. Es posible el tratamiento de datos sensibles cuando es necesario "para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento" (art. 9, lit. c), RGPD). Colombia y Uruguay mencionan el dato vital cuando se desarrolla las excepciones para el flujo transfronterizo de datos. Únicamente Costa Rica lo considera dato sensible.

En Ecuador, la única referencia a dato sensible consta en el artículo 92 de la Constitución relacionado con la acción constitucional de *habeas data*, por la cual su archivo deberá estar autorizado por la ley o por la persona titular; además, se exigirá la adopción de las medidas de seguridad necesarias.

Con esas consideraciones, la norma que regule datos sensibles para Ecuador, además de establecer su definición, debe considerarla especial y establecer un marco de protección reforzado, respecto de las condiciones para su tratamiento, las excepciones posibles y las medidas de seguridad que deben implementarse.

La normativa propuesta se concentra en un artículo de 6 que hace referencia a términos y definiciones, así como en el capítulo IV de categorías especiales de datos.

> Artículo 6.- Términos y definiciones.- Para los efectos de la aplicación de la presente Ley Orgánica se establecen las siguientes definiciones:
>
> *Anonimización:* La aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o re-identificación de una persona natural sin esfuerzos desproporcionados.
>
> *Base de datos:* Conjunto configurado, estructurado o no estructurado de datos, cualquiera que fuere la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento y acceso.

Consentimiento: Manifestación de voluntad libre, previa, específica, expresa, informada e inequívoca por la que el titular de los datos personales autoriza al responsable del tratamiento de datos personales a tratar los mismos.

Dato biométrico: Dato personal único obtenido a partir de un tratamiento técnico-específico, relativo a las características físicas, fisiológicas o conductuales de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.

Dato genético: Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo; generalmente se analizan a partir de muestras biológicas.

Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente, en el presente o futuro. Los datos inocuos, metadatos o fragmentos de datos que identifiquen o hagan identificable a un ser humano, forman parte de este concepto.

Datos personales crediticios: Datos que integran el comportamiento de personas naturales para analizar su capacidad de pago y financiera.

Datos personales registrables: Datos personales que conforme al ordenamiento jurídico deben estar contenidos en Registros Públicos.

Datos sensibles: Se consideran datos sensibles los relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos humanos o la dignidad e integridad de las personas. La Autoridad de Protección de Datos Personales podrá determinar otras categorías de datos sensibles.

Destinatario: Persona natural o jurídica que ha recibido comunicación de datos personales.

Disociación de datos: Todo tratamiento de datos personales destinado a que éstos no puedan ser asociados o vinculados a una persona identificada o identificable.

Elaboración de perfiles: Todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos de una persona natural para determinar comportamientos o patrones relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, ubicación, movimiento físico de una persona, entre otros.

Encargado del tratamiento de datos personales: Persona que trate datos personales por nombre y a cuenta de un responsable de tratamiento de datos personales.

Estado de la técnica: Estado último de cualquier particularidad que permita establecer bases de comparación para determinar si los requisitos o herramientas de carácter

administrativo, físico, técnico, organizativo, jurídico u otros constituyen niveles adecuados de protección en el tratamiento de datos personales.

Filtración: Es un incidente ilegal o no autorizado que involucra la visualización, acceso, extracción o divulgación de datos personales por un individuo, aplicación, servicio u otros.

Fuentes accesibles al público: Bases de datos que pueden ser consultadas por cualquier persona natural o jurídica, pública o privada, nacional o internacional cuyo acceso no se encuentre limitado por la normativa vigente o disposición de la Autoridad de Protección de Datos Personales.

Responsable del tratamiento de datos personales: Persona que decide sobre la finalidad y el tratamiento de datos personales.

Política de tratamiento de datos personales: Documento físico, electrónico o en cualquier formato generado por el responsable del tratamiento de datos personales que debe obligatoriamente ponerse a disposición del titular, a partir del momento en el cual se recaben sus datos personales y debe estar disponible de forma permanente, con el objeto de garantizar el derecho a la transparencia, cuyo contenido será definido por la Autoridad de Protección de Datos Personales.

Tercero: Persona que no ostenta la calidad de responsable o encargado de tratamiento; titular; o, Autoridad de Protección de Datos Personales, conforme al alcance establecido en la presente Ley.

Titular: Persona natural cuyos datos son objeto de tratamiento.

Transferencia o comunicación: Manifestación, declaración, publicación, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que han de comunicarse deben ser exactos, completos y actualizados.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, comunicación por transmisión, transferencia, difusión, procesamiento, almacenamiento, distribución, cesión, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.

Vulneración de la seguridad de los datos personales: Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales, como por ejemplo la filtración.

> Artículo 34.- Categorías especiales de datos personales.- Se aplicará lo dispuesto en el presente capítulo al tratamiento de datos sensibles, datos de niñas, niños y adolescentes, datos crediticios, datos de salud y datos necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística.

2.4 Sujeto activo

Por cuanto, la protección de datos personales se concibe como un derecho humano, su titular es la persona natural. El sujeto activo es el titular del derecho. Se excluye a las personas jurídicas, argumentando que este es un derecho fundamental que pertenece exclusivamente a las personas físicas, y que las personas jurídicas están reguladas por otras leyes como las de sociedades, patentes, marcas, defensa de la competencia, etc. Tampoco es considerado sujeto activo las empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto; tampoco empresarios individuales.

En los considerandos (2) y (14) del RGPD se utiliza la expresión "*derechos de los interesados*", y en varias referencias se utiliza el término "*interesado*". Esto para evitar utilizar términos como ciudadano, o residente puesto que por tratarse de un derecho fundamental no puede existir ninguna condición preexistente para que se considere titular a una persona.

También están dentro del ámbito de protección, independientemente de su "carácter notorio o público, pues, en muchos casos, es frecuente su aparición en prensa especializada u otros medios de comunicación",[1694] aquellas personas de contacto que pese a representar a la empresa como gerentes, representantes legales, directivos, etc., han entregado datos de carácter personal con total separación de su calidad de empresarios. Así lo ha señalado la SAN recurso 3517/2000/, 29 de septiembre 2001, que sigue la doctrina impuesta por el Tribunal Constitucional en STC 292/2000, 30 de noviembre,[1695] que dice: "*el carácter notorio de un dato personal no determina la* inaplicación al mismo de la LOPD y, por tanto, no puede admitirse que dicho dato pueda tratarse sin consentimiento del afectado. Excluir de la protección legal aquellos datos públicos y notorios implicaría establecer peligrosas excepciones a la tutela de derecho fundamentales".

Además, puede ocurrir también que los datos que se recaben sean de clientes-empresarios individuales, autónomos o profesionales, "personas jurídicas al fin y al cabo, pero revestidos de cierto velo jurídico en su actividad profesional",[1696] y que por su calidad de empresarios no están protegidas. No obstante, la AEPD ha señalado ciertas consideraciones:

[1694] N. SÁNCHEZ MOURIS, "Los datos personales en el inicio de la actividad empresarial", en *La Protección de Datos en la Gestión de Empresas*, dir. Ana Marzo Portera y Fernando Ramos (Navarra: Editorial Thomson - Aranzadi, 2004), 49.

[1695] La sentencia también dice: "el derecho fundamental a la protección de datos alcanza a [...] aquellos datos que por el hecho de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos... el que los datos sean de carácter personal no significa que sólo tenga protección los relativos a la vida privada o íntima de la persona sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de una persona".

[1696] A. QUINTANA, "La Protección de Datos en la Gestión de Empresas", *Revisa Aranzadi de derecho y Nuevas Tecnologías* (Navarra: Thomson-Aranzadi, 2004), 33.

1. Cuando se trata de *comerciantes, profesionales y empresarios individuales* la protección conferida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, no es aplicable a las personas jurídicas, que no gozarán de ninguna de las garantías establecidas en la Ley, y por extensión lo mismo ocurrirá con los profesionales que organizan su actividad bajo la forma de empresa (ostentando, en consecuencia la condición de comerciante a la que se refieren los artículos primero y siguientes del Código de Comercio) y con los empresarios individuales que ejercen una actividad mercantil de su propia actividad privada, estando en primer caso excluidos también del ámbito de aplicación de la Ley Orgánica 15/1999. En definitiva pues, tanto las personas jurídicas como los profesionales y los comerciantes individuales (estos dos últimos sólo en los estrictos términos señalados en el párrafo que antecede, esto es, cuando sus datos hayan sido tratados tan sólo en su consideración de empresarios) quedan fuera del manto protector de la Ley Orgánica 15/999.[1697]

   En consecuencia, cuando se utilicen datos de comerciantes, profesionales y empresarios individuales en una relación B2B, estos carecen de la protección que brinda la LOPD; no ocurre lo mismo si es que la relación es B2C porque, aun cuando se trata de una relación comercial, no se la realiza considerándoles empresarios sino consumidores, por tanto, los datos que faciliten son de carácter personal pues permiten identificarlos y desarrollar perfiles de personalidad, como por ejemplo cuando se somete sus datos a tratamientos tendientes a identificar un nicho de mercado susceptible de aprovechamiento económico por la empresa, junto con los datos de otros clientes, mediante procesos de segmentación geo demográficos.

   Lo fundamental entonces es "ir analizando caso por caso para hallar en cada supuesto concreto el límite fronterizo donde resulte afectado el derecho fundamental a la protección de datos de los interesados personas físicas, o, por el contrario, aquél no resulte amenazado por incidir tan solo en la esfera de la actividad comercial o empresarial, teniendo en todo caso presente que, en caso de duda, la solución deberá siempre adoptarse a favor de la protección de los derechos individuales",[1698] tal como señala la AEPD.

   Solo el análisis de las particularidades de cada caso, permite identificar si un empresario individual tiene derecho o no a la protección de sus datos de carácter personal, sobre todo ante la vulneración de otros derechos fundamentales de los que es titular en su calidad de persona física, independientemente de su distintivo de comerciante.

2. Cuando se trata de *profesionales autónomos o profesiones liberales* "A contrario sensu", tanto los profesionales como los comerciantes individuales quedarían bajo el ámbito de aplicación de la Ley Orgánica 15/1999 y, por tanto, amparados por ella cuando los primeros no tuvieran organizada su actividad profesional bajo la forma de empresa, no

[1697] Memoria de la Agencia Española de Protección de Datos correspondiente al ejercicio 2001, Consulta sobre el Ámbito Subjetivo de Aplicación de la Ley Orgánica 15/1999, 13 de diciembre, de Protección de Datos de Carácter Personal, accedido 1 de junio del 2007, https://www.agpd.es/upload%2FCanal_Documentacion%2FInformes%20Juridicos%2FAmbito%20de%20Aplicacion%2FA%20%282001-0000%29%20%28%E1mbito%20subjetivo%20de%20la%20aplicaci%F3n%20de%20la%20LOPD%29.pdf.
[1698] Ibíd.

> ostentando, en consecuencia, la condición de comerciante (es el caso de los profesionales liberales cuyas actividades están expresamente excluidas del ámbito de aplicación de la Ley Básica 3719993 por su artículo 6) y los segundos cuando no fuera posible diferenciar su actividad mercantil de la propia actividad privada. En estos dos casos deberán aplicarse siempre las garantías de la Ley Orgánica 15/1999 dada la naturaleza fundamental del derecho a proteger".[1699]

La razón de esta protección limitada se debe, según el Tribunal de Justicia, a que "para las personas jurídicas, la gravedad de la lesión del derecho a la protección de sus datos de carácter personal se presenta de modo diferente que para las personas físicas". Y este argumenta que, en el caso específico de la publicación de información de beneficiarios de ayudas públicas, la razón de esta diferencia se debe a que "las personas jurídicas ya están sometidas a una obligación acrecentada de publicación de los datos que les conciernen". Ver apartado 87 de la sentencia de 20 de mayo de 2003, Osterreichischer Rundfunk y otros, asuntos acumulados C.465/00, C-138/01 y C-139/01.[1700]

En algunos países latinoamericanos se señala la frase generalizada "toda persona": Argentina, Perú, Colombia, Nicaragua, República Dominicana, Panamá y Guatemala (esta última, desde su visión limitada de carácter sectorial atinente únicamente a lo público). Ecuador, Uruguay y Costa Rica no utilizan la locución citada, pero se refieren a las personas en general. Finalmente, México utiliza el enunciado general "toda persona" y precisa que el titular no requiere la necesidad de que se acredite interés alguno o se justifique su utilización.

Esta forma de abordar la norma, lejos de clarificar que solo la persona natural es titular del derecho, lleva a concluir que por regla general no se acepta como titular del derecho a la protección de datos personales a las personas jurídicas, sean estas públicas o privadas; pero que existen países donde esta posibilidad existe: Panamá, Colombia, únicamente respecto de la solicitud de información en ejercicio de sus funciones legales o por orden judicial. Mientras que en Uruguay, Perú, Panamá, Ecuador, Colombia, Nicaragua y Argentina se reconocen como titulares a personas jurídicas privadas, atendiendo cada caso.

Ecuador reconoce como titulares a comunidades, pueblos, nacionalidades y colectivos; procede de datos propios y distintos de los miembros.

Conforme el considerando (27), el RGPD tampoco aplica al tratamiento de los datos personales de fallecidos, cuyos titulares serán sus herederos universales. En el mismo sentido, la normativa de Argentina, Costa Rica, México, Nicaragua, República Dominicana y Uruguay.

Cabe anotar que la normativa mexicana menciona que es necesario acreditar interés jurídico, de conformidad con las leyes aplicables, y siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto (art. 49, *Ley de Sujetos Obligados*, México).

Sobre un grupo de especial protección como son los niños, el considerando (38) del RGPD establece limitaciones a "la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de

[1699] Ibíd.
[1700] J. PIÑAR MAÑAS y M. RECIO GAYO, *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea* (España: La Ley, 2018).

datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños".

Por su lado, la normativa peruana reconoce un régimen especial para los datos de niños y adolescentes que deberá ser desarrollado en un reglamento que permita la protección y garantía de sus derechos. "Para el ejercicio de los derechos que está Ley reconoce, los niños y los adolescentes actúan través de sus representes legales, pudiendo el reglamento determinar las excepciones aplicables de ser el caso, teniendo en cuenta para ello el interés superior del niño y del adolescente" (art. 13.3, Ley 29733).[1701]

Por su parte, Colombia señala que el tratamiento de datos personales de niños, niñas y adolescentes queda proscrito, salvo aquellos datos que sean de naturaleza pública. Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer conocimiento que verse acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás (art. 7º, Ley 1581).[1702] Asimismo, el responsable del tratamiento, al momento de solicitar al titular la autorización, deberá informarle de manera clara y expresa lo siguiente: b. El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes (art. 12, Ley 1581).[1703]

Finalmente, República Dominicana, en el artículo 79 de la Ley 29733,[1704] señala que el tratamiento de datos de menores de edad estará formado por las disposiciones establecidas en el Código para la Protección de los Derechos de los Niños, Niñas y Adolescentes, el Código Penal y otras leyes especiales.

En Ecuador, como se analizó en el primer capítulo de este trabajo de investigación, queda claro que debido al contenido del artículo 10 de la Constitución es titular de derechos fundamentales, tanto la persona natural como la persona jurídica; sin embargo, deberá revisarse en cada caso la titularidad del derecho reclamado en cada caso puesto en conocimiento de la Corte Constitucional, que es el máximo organismo de justicia constitucional en Ecuador. Asimismo, la titularidad de derechos a comunidades, pueblos y nacionalidades en las que nuevamente este órgano máximo deberá pronunciarse de presentarse el caso específico.

De otro lado, los niños, niñas y adolescentes serán grupo de atención prioritaria y para su protección se ha instituido el principio de interés superior, por lo que se debe acoger las iniciativas europeas y latinoamericanas que protejan sus datos personales, mediante prohibiciones y controles.

Finalmente, no son titulares de derechos los fallecidos pero si lo serán sus herederos, por lo que esta aclaración también debe constar en una norma que establezca quienes son los sujetos activos de este derecho fundamental. El término titular se ve definido en el artículo 6 de

[1701] Congreso de la República del Perú, *Ley 29733, de Protección de Datos Personales*.
[1702] *Ley protección de datos personales (Ley 1581 de 2012)* - vLex Global.
[1703] Ibíd.
[1704] Congreso de la República del Perú, *Ley 29733*.

términos y definiciones, para el caso de personas fallecidas el tratamiento de esta categoría especial se aplica conforme el artículo 38 de la normativa propuesta.

> **Artículo 6.- Términos y definiciones.-** Para los efectos de la aplicación de la presente Ley Orgánica se establecen las siguientes definiciones: (…) *Titular:* Persona natural cuyos datos son objeto de tratamiento.
>
> **Artículo 38.- Datos de personas fallecidas.-** Los titulares de derechos sucesorios del fallecido podrán dirigirse al responsable del tratamiento de datos personales con el objeto de solicitar el acceso, rectificación y actualización o eliminación de los datos personales del causante.
>
> Las personas o instituciones que el fallecido haya designado expresamente para ello, podrán también solicitar con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste; y, en su caso su rectificación, actualización o eliminación.
>
> En caso de fallecimiento de niñas, niños, adolescentes o personas a las que la Ley reconoce como incapaces, estas facultades podrán ejercerse por quién hubiese sido su último representante legal.

2.5 Sujeto pasivo

Según señala el considerando (74) del RGPD, son sujetos pasivos aquellos a quienes la citada norma obliga al cumplimiento de la normativa y medidas oportunas y eficaces y demostrables de sus actividades de tratamiento, y en caso de no cumplir responsabiliza directamente; incluso con indemnizaciones si se llegaren a producir daños por su acción u omisión.

Los sujetos pasivos reconocidos el RGPD, los Estándares Iberoamericanos de Protección de Datos Personales y varios de los países latinoamericanos son:

e) *Responsable de tratamiento o simplemente responsable*. Tanto la normativa europea como latinoamericana coinciden en señalar que es la persona física o jurídica, autoridad pública o privada, servicio u otro organismo que, solo o junto con otros, determina los fines o finalidad, medios, contenido o uso del tratamiento.

   Este contenido casi idéntico consta en el artículo 4, numeral 8) del RGPD; artículo 2, literal g) de los Estándares Iberoamericanos de Protección de Datos Personales; artículo 2 de la Ley 25.326 del Argentina;[1705] artículo 3 de la Ley 1581 de Colombia;[1706] artículo 3, literal h de la Ley 8968 de Costa Rica;[1707] artículo 3, Ley 787-2012 de Nicaragua;[1708] artículo 3 XXVIII de la ley que regula sujetos obligados de México,[1709] y artículo 3 XIV de la ley que regula particulares.[1710] Artículo 15,

[1705] Congreso de la República Argentina, *Ley 25.326 de Protección de los Datos Personales*.
[1706] *Ley protección de datos personales (Ley 1581 de 2012)* - vLex Global.
[1707] Asamblea Legislativa de la República de Costa Rica, *Ley de Protección de la Persona frente al tratamiento de sus datos personales 8968*, 7 de julio de 2011.
[1708] *Ley 787, Ley de Protección de Datos Personales de Nicaragua*, 29 de marzo de 2012 - vLex Global.
[1709] Congreso de la Unión de Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en posesión de sujetos obligados*.

numeral 2 de la Ley 29733 del Perú, lo denomina titular de la base o bando de datos en lugar de responsable;[1711] artículo 6, numeral 18 de la Ley 172-13[1712] de República Dominicana; y artículo 4, literal k) de la Ley 18331 del Uruguay.[1713]

Conforme la STS español, de 3 de diciembre de 2002, recurso 7050/2001 respecto de las características que definen al responsable del fichero dice: "es quien decide sobre la finalidad, contenido y uso del tratamiento automatizado y no quien le facilita el dato en virtud de un contrato celebrado con aquel, de modo que solo el responsable del fichero está sujeto al régimen sancionador".

f) *Encargado del tratamiento o simplemente "encargado".* Nuevamente tanto el RGPD como en la mayoría de la normativa latinoamericana, la definición de encargado es la persona física o jurídica, autoridad pública o privada, servicio u otro organismo, que por sí misma o en asocio con otros, trate datos personales por cuenta del responsable del tratamiento (art. 4, núm. 8), RGPD; y art. 2, lit. e), Estándares Iberoamericanos de Protección de Datos Personales).

Contenido similar consta en el artículo 3, literal d) de la Ley 1581 de Colombia;[1714] artículo 9, Ley 787-2012 de Nicaragua;[1715] artículo 3 XV de la Ley que regula sujetos obligados de México,[1716] y artículo 3 IX de la Ley que regula particulares.[1717] Artículo 6, numeral 2 de la Ley 29733 del Perú;[1718] artículo 6, numeral 12 de la Ley 172-13[1719] de República Dominicana; y artículo 4, literal h) de la Ley 18331 del Uruguay.[1720] Argentina no recoge la figura del encargado.

g) *Destinatario.* Es la persona física o jurídica, autoridad pública, servicio u otro organismo a la que se comuniquen datos personales, se trate o no de un tercero (art. 4, núm. 9), RGPD), pero excluye a los destinatarios públicos en el marco de sus competencias legales. República Dominicana señala el mismo concepto, pero señala que es al que se le revelen datos (art. 6, núm. 11, Ley 172-13[1721] de República Dominicana). Mientras que Uruguay señala que al que recibiere comunicación (art. 4, lit. f), Ley 18331 del Uruguay).[1722] En cualquiera de los casos, es evidente que el

---

[1710] Congreso General de los Estados Unidos Mexicanos, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*».
[1711] Congreso de la República del Perú, *Ley 29733, de Protección de Datos Personales*, 3 de julio de 2011
[1712] Congreso Nacional de República Dominicana, *Ley 172-13*.
[1713] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, *Ley 18.331 de Protección de Datos Personales y Acción de Habeas Data*, 11 de agosto de 2008, D.O. 18 ago/008 - 27549.
[1714] *Ley protección de datos personales (Ley 1581 de 2012)* - vLex Global.
[1715] *Ley 787, Ley de Protección de Datos Personales de Nicaragua*, 29 de marzo de 2012 - vLex Global.
[1716] Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en posesión de sujetos obligados*.
[1717] Congreso General de los Estados Unidos Mexicanos, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*.
[1718] *Congreso de la República del Perú, Ley 29733, de Protección de Datos Personales*, 3 de julio de 2011
[1719] Congreso Nacional de República Dominicana, *Ley 172-13*.
[1720] El Senado y la Cámara de Representantes de la República Oriental del Uruguay *Ley 18.331*.
[1721] Congreso Nacional de República Dominicana, *Ley 172-13*.
[1722] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, *Ley 18.331*.

concepto es muy similar pues tiene por objetivo proteger los datos personales por la simple condición de que han llegada a su conocimiento.

h) *Tercero*. Es la persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado (art. 4, núm. 9), RGPD). No consta la figura del tercero en los Estándares Iberoamericanos.

La normativa latinoamericana señala que el tercero trata los datos bajo la autoridad directa del responsable o del encargado del tratamiento: México, artículo 3 XVI de la ley que regula particulares;[1723] artículo 6, numeral 19 de la Ley 172-13[1724] de República Dominicana, y artículo 4, literal j) de la Ley 18331 del Uruguay.[1725]

i) *Usuario de datos.* Es el equivalente a responsable ya que es toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos: artículo 2, Ley 25.326 de Argentina;[1726] artículo 6, numeral 49, Ley 172-13[1727] de República Dominicana, y artículo 4, literal n), Ley 18331 del Uruguay.[1728]

j) *Exportador*. El exportador como sujeto pasivo consta en el artículo 2 de los Estándares Iberoamericanos de Protección de Datos Personales; consiste en la persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situados en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes estándares. En igual sentido, consta en el artículo 6, numeral 13, Ley 172-13[1729] de República Dominicana.

k) *Importador de datos personales.* El artículo 6, numeral 15 de la Ley 172-13[1730] de República Dominicana señala como sujeto pasivo también al importador; esto es la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos, en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

El artículo 4, literal 16 del RGPD establece varios criterios que ayudan a comprender el contenido de la normativa que regula a los sujetos pasivos; estos son:

f) *Establecimiento principal*, por el cual será responsable del tratamiento el que tenga un establecimiento en más de un Estado miembro, el lugar de su administración central en la Unión; salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión. Y este último establecimiento tenga el poder de

[1723] Congreso General de los Estados Unidos Mexicanos, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*.
[1724] Congreso Nacional de República Dominicana, *Ley 172-13*.
[1725] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, *Ley 18.331*.
[1726] Congreso de la República Argentina, *Ley 25.326 de Protección de los Datos Personales.*
[1727] Congreso Nacional de República Dominicana, *Ley 172-13*.
[1728] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, *Ley 18.331*.
[1729] Congreso Nacional de República Dominicana, *Ley 172-13*.
[1730] Ibíd.

hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal; será *encargado del tratamiento* con establecimientos en más de un Estado miembro. El lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al RGPD.

g) *Representante.* El artículo 4, numeral 17, establece que se entenderá como representante a la "persona física o jurídica que ha sido designada por escrito por el responsable o el encargado del tratamiento, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones".

h) *Empresa o grupo empresarial.* El artículo 4, numeral 18, establece que una empresa será la persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica"; y grupo empresarial el constituido por una empresa que ejerce el control y sus empresas controladas (art. 4, num. 19, RGPD).

Del análisis realizado, es importante que la normativa ecuatoriana recoja al menos los sujetos pasivos más importantes: el responsable del tratamiento, el tercero y el destinatario. No debería incluirse ni la figura del usuario de datos ni del exportador ni del importador con la finalidad de no causar confusión, ya que el primero equivale a responsable y los dos restantes se utilizan exclusivamente para flujo transfronterizo de datos.

> ***Artículo 6.- Términos y definiciones.-*** *Para los efectos de la aplicación de la presente Ley Orgánica se establecen las siguientes definiciones:*
>
> *Responsable del tratamiento de datos personales*: Persona que decide sobre la finalidad y el tratamiento de datos personales.
>
> *Tercero:* Persona que no ostenta la calidad de responsable o encargado de tratamiento; titular; o, Autoridad de Protección de Datos Personales, conforme al alcance establecido en la presente Ley.
>
> *Encargado del tratamiento de datos personales:* Persona que trate datos personales por nombre y a cuenta de un responsable de tratamiento de datos personales.

2.6 Objeto o bien jurídico

2.6.1 Derecho de información

Conforme consta en el RGPD, las personas son titulares del derecho de información directamente relacionado con la protección de datos personales, pues atiende a las prerrogativas que tienen las personas de conocer la existencia, la finalidad de un fichero, quién es su responsable, su domicilio, dónde realizar los reclamos, entre otros.

Se añaden aquellos elementos que han sido recogidos en la normativa europea; es decir, del artículo 12 del RGPD —que hace alusión a que es derecho recibir información sobre las modalidades de ejercicio de los derechos del interesado— las medidas oportunas que el interesado puede tomar, sobre todo, para solicitar el ejercicio de los Derechos ARCO, así como la forma en la que se realizará el tratamiento; que además deberá comunicarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, de forma gratuita, por escrito, por medios electrónicos o incluso verbalmente.

En los países latinoamericanos, sobre el derecho de información únicamente Panamá y Costa Rica no lo reconocen como derecho, sino como condición para la eficacia del consentimiento informado.

Argentina, Colombia, México, Nicaragua, Perú, República Dominicana y Uruguay consagraran el derecho de información sobre los datos o la existencia de la base de datos o registro, la finalidad del procesamiento, el uso o tratamiento, así como la identidad de los destinatarios, responsables, encargados, sean estos personas públicas o privadas. Además, el carácter facultativo de las respuestas, sobre todo, en caso de datos sensibles o sobre niños, niñas o adolescentes; los derechos que le asisten como titular, es decir derechos ARCO; la obligación de conservar prueba del cumplimiento; el tiempo de vigencia y el aviso de privacidad tanto si son recogidos en línea o no.

En la normativa ecuatoriana no consta descrito este derecho en el artículo 66 de la Constitución, pero si aparece en el artículo 92 de la citada normativa, que se refiere a la acción constitucional de *habeas data*, y en el artículo 49 de la LOGJCC, también referente a esta acción. Allí se menciona que toda persona tendrá derecho a conocer de la existencia, finalidad, origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Es decir, se reconoce no solo como deber o principio el de información, sino como derecho de la persona titular del dato personal.

De ese modo, debe constar en una propuesta de normativa este contenido específico por disponerlo la propia Constitución ecuatoriana.

> Artículo 21.- Derecho a la lealtad, transparencia e información.- El titular de datos personales tiene derecho a ser informado de forma leal y transparente por cualquier medio sobre:
>
> a) Los fines del tratamiento;
>
> b) Base legal para el tratamiento;

c) Tipos de tratamiento;

d) Tiempo de conservación;

e) La existencia de una base de datos en donde consten sus datos personales;

f) El origen de los datos personales cuando no se hayan obtenido directamente del titular;

g) Otras finalidades y tratamientos ulteriores;

h) Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluye: dirección de domicilio legal, número de teléfono y correo electrónico;

i) Identidad y datos de contacto del delegado de protección de datos personales, que incluye: dirección domiciliaria, teléfono y correo electrónico;

j) Las transferencias o comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de las mismas;

k) Carácter obligatorio o facultativo de la respuesta y las consecuencias de proporcionar o no sus datos personales;

l) El efecto de suministrar datos personales erróneos o inexactos;

m) La posibilidad de revocar el consentimiento;

n) La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas;

o) Los mecanismos para hacer efectivo su derecho a la portabilidad, cuando el titular lo solicite;

p) Donde y como realizar sus reclamos ante el responsable del tratamiento de datos personales y la Autoridad de Protección de Datos Personales; y,

q) La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles.

En el caso que los datos fueran obtenidos directamente del titular, la información deberá ser comunicada de forma previa a éste es decir, en el momento mismo de la recogida del dato personal.

Excepcionalmente, el titular deberá ser informado de forma posterior, dentro del mes siguiente, cuando los datos personales no se obtuvieren de forma directa; expresa; transparente; inteligible; concisa; precisa; sin barreras técnicas; e, inequívoca.

Con el objeto de que pueda autorizar el tratamiento, transferencia o comunicación de sus datos personales, esta información deberá ser proporcionada al titular de forma accesible por cualquier medio, incluidas políticas de protección de datos personales; gratuitos; suficientes; disponibles de forma permanente y redactarse en un lenguaje claro; sencillo; y, de fácil comprensión incluso cuando se trate de contratación electrónica.

En el caso de productos o servicios dirigidos, utilizados o que pudieran ser utilizados por niñas, niños y adolescentes, la información a la que hace referencia el presente artículo será proporcionada a su representante legal conforme a lo dispuesto en el inciso precedente.

2.6.2 Autodeterminación informativa

Según se analizó en los capítulos precedentes, el derecho a la autodeterminación informativa ha sido considerado parte del contenido esencial del derecho a la protección de datos personales ya que las personas tienen derecho a decidir sobre la entrega de su información personal. Es un derecho de acción a diferencia del derecho a la intimidad del cual se independizó precisamente por la postura positiva que plantea.

Además, el titular tiene derecho a negarse a entregar sus datos a un particular e incluso al Estado, si no se encuentra autorizada por la ley. Puede decidir sobre si permitir que sus datos sean conservados, tratados, cedidos o utilizados para finalidades distintas para las que fueron recogidos.

Para el Tribunal Constitucional Federal Alemán (TCFA), en la sentencia sobre la Ley de Censo, "la autodeterminación del individuo presupone —también en las condiciones de las técnicas modernas de tratamiento de la información— que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso, a omitir incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada".[1731]

El autor Ricard Martínez señala que:

> [...] la libertad de decisión, de control, supone además que el individuo tenga la posibilidad de acceder a sus datos personales, que pueda, no solo tener conocimiento de que otros procesan informaciones relativas su persona, sino también someter el uso de éstas a un control, ya que, de lo contrario, se limitará su libertad de decidir por autodeterminación no es posible la compatibilidad de un orden social y del ordenamiento jurídico que lo sostiene si el individuo no puede conocer quién, cuándo y que motivo cataloga, utiliza o trasmite la información personal que le pertenece.[1732]

En el capítulo cuarto de este trabajo de investigación se concluyó que no existe unanimidad sobre hasta dónde llega el poder de decisión del titular, puesto que en el caso argentino[1733] aún se limita esta libertad a la naturaleza errónea o discriminatoria del dato o su tratamiento y no a la simple voluntad del titular. La mayoría de países latinoamericanos conciben legal o

[1731] Traducida por M. DARANAS, en BJC, núm. 33, enero de 1984. Véase M. HEREDERO HIGUERAS: La sentencia del Tribunal Constitucional de la República Federal Alemana relativa al censo de población de 1983, en Documentación Administrativa, núm. 198, 1993, págs. 139-158 citado por Ricard Martínez Martínez, *Una aproximación crítica a la autodeterminación informativa* (Madrid: Civitas, 2004).
[1732] MARTÍNEZ MARTÍNEZ, ibíd.
[1733] Artículo 43 de la Constitución argentina de 1994: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística".

jurisprudencialmente[1734] a la autodeterminación informativa como un elemento sustancial del derecho a la protección de datos personales.

De las referencias legales al concepto de autodeterminación informativa, la más completa es la contenida en la Ley 8968 de Costa Rica, que determina que se garantiza a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad; así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Otro país que recoge una referencia clara sobre autodeterminación informativa es México, ya que el artículo 16 de su Constitución determina que toda persona tiene derecho al acceso, rectificación y cancelación, y a oponerse a la recopilación o tratamiento de sus datos, excepto en los casos expresamente autorizados por la ley. En el mismo sentido, el artículo 1 de la LFPDPPP de 2010 señala que esta tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Entretanto, la autodeterminación informativa como derecho fundamental se encuentra recogida en el numeral 19 del artículo 66 de la Constitución ecuatoriana, cuando incluye entre los derechos que son parte de la protección de datos personales a la "decisión sobre información y datos de este carácter". Asimismo, la jurisprudencia dictada por la Corte Constitucional ecuatoriana, sentencia 001-14-PO-CC, 3 de julio de 2014, establece a la autodeterminación informativa, como parte del derecho a la protección de datos personales, esto es la posibilidad de ejercer control sobre sus datos personales, incluso cuando estos no se encuentren en su poder.

En consecuencia, es indispensable que en el objetivo de la ley se establezca a la autodeterminación informativa debidamente dimensionada; en otras palabras, la posibilidad de decidir sobre todos los aspectos relacionados con los datos personales.

De modo que se incluya en la normativa los derechos de acceso, rectificación, cancelación y oposición, así como respecto de otras características más específicas propias del almacenamiento o tratamiento de datos personales. No es suficiente la mención a la autodeterminación informativa, sino su puesta en vigencia en cada uno de las fases del ciclo del dato.

2.6.3 Necesidad de mandato legal para tratamiento sin autorización del titular

Tanto en la normativa europea como en la latinoamericana el eje del sistema de protección de los datos personales es el consentimiento informado. El artículo 6 del RGPD delinea la licitud del tratamiento, al establecer las condiciones necesarias para que se pueda producir un tratamiento de datos personales, es decir el previo consentimiento informado del interesado en uno o varias finalidades. Así como, la ejecución de un contrato o la aplicación de medidas

[1734] Corte Constitucional de Colombia, "Sentencia C-748/11", 10 de junio de 2011, http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm.

precontractuales, el cumplimiento de una obligación legal aplicable al responsable, la protección de un interés vital, el cumplimiento de una misión de interés público o inherente al ejercicio del poder público, o satisfacción de un interés legítimo, especialmente cuando el interesado sea un niño. La base del tratamiento y la finalidad deberá constar de forma específica en la normativa pertinente cuando se verifica para el cumplimiento de una obligación legal o de una misión de interés público o inherente al ejercicio del poder público y será proporcional al fin legítimo perseguido. Se determinará en especial las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas.

Finalmente, cuando el tratamiento sea para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en disposición legal que autorice en su lugar, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta: la relación entre los fines previos y ulteriores; el contexto en que se hayan recogido los datos personales; la naturaleza de los datos personales, en concreto las categorías especiales de datos personales; las posibles consecuencias para los interesados del tratamiento ulterior previsto; la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización (art. 6, RGPD).

Respecto de los datos necesarios dentro de una relación precontractual o contractual, se aclara que son aquellos como nombres, dirección, teléfono, DNI (solo si es que forman parte de una clave de acceso a un sistema de identificación vía telefónica o página web), datos económicos-financieros; es decir, aquellos que permiten la identificación de las partes, el mantenimiento y el cumplimiento del contrato.

Por el contrario, no son datos necesarios para cumplir y mantener una relación negocial los relativos a características personales, académicas, profesionales, circunstancias sociales, preferencias, hobbies, etc.; sin embargo, son imprescindibles cuando una empresa quiere aplicar estrategia de marketing relacional, ya que son los que se utilizan dentro de las fases finales del ciclo del cliente, cuando la empresa pretende satisfacerle y retenerle.

De lo dicho, se concluye que cuando la empresa requiera de datos para propósitos distintos a los transaccionales, no puede excepcionarse de recoger el consentimiento del cliente bajo su supuesta necesidad dentro de una relación negocial más amplia, denominada “satisfacción y retención del cliente”, ya que su indeterminación impediría el cumplimiento de otro de los requisitos del consentimiento, el de especificidad; además de la transgresión a los principios de calidad de datos acerca de su adecuación, pertinencia y finalidad; y al de información sobre las finalidades.

Además, la necesidad del consentimiento en el marco de las relaciones contractuales o precontractuales debe caminar junto al principio de datos adecuados, pertinentes y no excesivos con el ámbito y las finalidades para los que fue inicialmente obtenido. De esta forma, los datos que no sean necesarios para estos fines deberán contar con la cobertura del consentimiento.

Es posible el uso de datos personales cuando estos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Esta excepción se aplica generalmente por las "*empresas de publicidad que se dedican a recabar datos de carácter personal de fuentes accesibles al público bien para realizar envíos publicitarios, bien para venderlos a otras empresas que los destinen a los mismos fines. En este caso no es necesario contar con el consentimiento de los interesados, pero sí informales de la finalidad de la recogida de datos*"[1735]. Como vemos, la empresa que utiliza ficheros públicos, además de cumplir con el deber de información en cada comunicación que se realice con el cliente, debe también recabar de su consentimiento para el tratamiento actual de sus datos.

Respecto de la normativa latinoamericana, es necesario aclarar que al desarrollar la necesidad de mandato legal para el tratamiento de datos personales sin autorización del titular se establecía el ámbito de inaplicación de la normativa de protección de datos personales. Esta forma de concebir la normativa se debía a que por disposición legal se establecía la no aplicabilidad de la norma, y por lo tanto la posibilidad de tratar datos personales con los que se pudiera dar cumplimiento a las obligaciones legales relacionadas con seguridad y defensa nacional; así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo o que contengan información de inteligencia y contrainteligencia, al tenor la Ley 1581 de Colombia.

Lo mismo se plantea la normativa mexicana, cuyo artículo 117 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) establece la excepción relativa a razones de seguridad nacional y salubridad general, o para proteger los derechos de terceros. Determina la necesidad de prueba de interés público, y de proporcionalidad entre la invasión a la intimidad ocasionada por la divulgación de la información confidencial y el interés público de la información.

Cabe resaltar la postura peruana que establece que las limitaciones al ejercicio del derecho fundamental al derecho a la protección de datos personales solo podrán ser establecidas por ley, respetando su contenido esencial y justificarse en razón del respeto de otros derechos fundamentales.

Como se señaló previamente, el régimen se basa en el consentimiento informado, pero a falta de este debe existir disposición legal, pero además se añade la posibilidad de que se supla la autorización mediante orden judicial, la cual no está expresamente reconocida en la normativa europea, aunque podría extrapolarse de la condición relativa al cumplimiento de una obligación legal, pero como en la normativa latinoamericana esta aproximación no es precisa; es preferible añadir esta circunstancia de forma expresa.

Resta por precisarse que la licitud no solo se refiere al acceso, como erróneamente consta las normativa colombiana y mexicana, sino que incluye la recopilación, el tratamiento, divulgación, cesión, sino a todas aquellas condiciones generales que debe cumplir el responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación

[1735] SÁNCHEZ MOURIS, "Los datos personales en el inicio de la actividad empresarial", 63.

de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas de seguridad, al tenor de lo señalado en el artículo 6.3 del RGPD.

Se rescata del RGPD la posibilidad de tratar datos personales cuando los tribunales y otras autoridades judiciales cumplan con sus actividades, puesto que pueden por sí mismo especificar las operaciones de tratamiento y los procedimientos de tratamiento, con la finalidad de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones.[1736]

En el mismo sentido, en las autoridades públicas a las que se comunican datos personales debido a una obligación legal para el ejercicio de su misión oficial se incluyen las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, quienes no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, tal como señala el RGPD.

En suma, la normativa ecuatoriana debe diferenciar entre ámbitos de inaplicación que es plausible solo en aquellos casos en los que se justifica un completo alejamiento de los principios y derechos de los titulares de aquellos datos personales que ameritan ser tratados pero que no necesitan de autorización del titular, sino que la ley suple esta condición y es posible su tratamiento en aras de cumplir con finalidades de interés general que siendo proporcionales vayan en provecho de la sociedad y de los individuos y sus derechos fundamentales.

Para tal efecto, y por cuanto se ha desarrollado con mayor organicidad y lógica se puede acoger el modelo previsto en el RGPD que establece en el artículo 2 aquellos datos personales que no entran en el sistema de protección: los que no están comprendidos en una actividad reconocida por la Unión Europea; los datos relacionados con la política común de seguridad y defensa de la Unión Europea; los efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas; y los recogidos por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención.

Todos los otros datos, estos sean los históricos, estadísticos o científicos, siempre que estén disociados o anonimizados, los relativos a salud física o mental, de salud pública, de emergencia, urgencia médica o sanitaria o para la realización de estudios epidemiológicos. También aquellos que se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; los datos de naturaleza pública; los de registros públicos o accesibles al público, o relacionados con el Registro Civil de las Personas; aquellos necesarios para actividades legítimas por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical. Además, aquellos sobre seguridad pública o nacional u orden público, fines de fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; necesarios para la investigación de delitos, infracciones administrativas o infracciones de la deontología en las profesiones; el reconocimiento, ejercicio o defensa de un

[1736] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.

derecho en un proceso judicial; por orden judicial; contratación de servicios de terceros para tratamiento de datos; producto de una relación contractual, científica o profesional del titular de los datos, el giro de las actividades comerciales o crediticias de los cesionarios; las operaciones que realicen las entidades financieras, entre otros. En todos estos casos, no están por fuera del sistema de salvaguarda de los datos personales, por lo que la normativa le es plenamente aplicable.

Más bien, la precisión que se realiza sobre estos datos se refiere a la necesidad de autorización legal para su tratamiento sin autorización del titular, además de la existencia de marcos específicos de regulación en todo el ciclo del dato como garantía de los derechos de su titular, pero al mismo tiempo de respeto de las finalidades y de las relaciones jurídicas de los particulares, así como del cumplimiento de obligaciones legales y de interés público.

La necesidad de mandato legal que suple la autorización para tratar datos personales sin consentimiento, es imperiosa para garantizar el libre flujo de datos para entes privados en sus relaciones comerciales contractuales y precontractuales, facilitar el cumplimiento de las obligaciones legales; así como del interés público y de orden público que requiere del tratamiento de estos datos y su transmisión sin autorización del titular.

2.6.4 Principios

Es parte del contenido esencial del derecho a la protección de datos personales la inclusión de los principios que lo regentan. Tanto el RGPD, los Estándares Iberoamericanos de Protección de Datos Personales como la normativa latinoamericana que salvaguarda este derecho fundamental recogen la idea de principios. Únicamente varían respecto del tipo de principios, añadiendo varios, precisando su contenido y dotándolos de particularidades dependiendo de las condiciones específicas de cada entorno social donde se aplicará.

A continuación se recogerán aquellos principios cuyo contenido se entiende indispensable para garantizar un libre flujo informacional, y al mismo tiempo la garantía y respeto por los titulares de sus datos, su dignidad, sus libertades individuales y sus derechos fundamentales.

Se recalca que las peculiaridades de cada país latinoamericano y las distintas experiencias, sobre todo en el ámbito europeo, han marcado que su contenido se haya ampliado de sus versiones originales. Asimismo, se ha clarificado conceptos que han permitido el nacimiento de otros principios que provienen de formas iniciales de aproximación a ciertas temáticas. Por ejemplo, el principio de licitud que se diferencia del principio de legitimación y del principio de lealtad, cuyas diferencias se analizarán a continuación.

2.6.4.1 Del deber de información a la transparencia

Como la otra cara de una moneda, el deber de información es la respuesta al derecho de información. Puesto que los titulares tienen como parte del derecho a la protección de datos personales, la prerrogativa de exigir se le informe de la existencia de una base de datos, la finalidad de la recogida y tratamiento de datos, la identidad y datos generales del responsable, los mecanismos para realizar un ejercicio efectivo de los derechos ARCO, los mecanismos de seguridad, conservación y perdurabilidad del dato, entre otros. A *contrario sensu*, los

responsables tienen el deber de garantizar todos aquellos derechos de los que son titulares las personas naturales.

Como se analizó en el capítulo IV de este estudio, el deber de información se lo concibe como un derecho y también como un deber de los responsables de tratamiento, por lo que la normativa de Argentina, Costa Rica, México, Nicaragua, Perú, República Dominicana, Uruguay desarrollan ampliamente su contenido. La excepción es Colombia que en el literal e) del artículo 4º de la Ley 1581 de 2012, de la Ley de Protección de Datos Personales, establece la obligación de que el Gobierno nacional establezca la forma en la cual los responsables y encargados del Tratamiento suministren la información del titular, dejando al organismo público la determinación de tales condiciones. Y en el caso de Guatemala, la normativa[1737] se limita a la obligación de capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos.

Ahora bien, tanto el RGPD como en los Estándares Iberoamericanos además de listar al deber de información como una de las obligaciones del responsable del tratamiento, y a *contrario sensu*, su contenido, ámbito y alcance constan reconocidos en un derecho de los titulares que al mismo tiempo es un principio del tratamiento, denominado transparencia de la información y de la comunicación y que incluye hasta las modalidades de ejercicio de los derechos del interesado. La transparencia como derecho consta en el artículo 12 del RGPD y como principio de tratamiento en el artículo 5 del mismo reglamento. Por su parte, se reconoce a la transparencia únicamente como principio en el estándar iberoamericano en el número 16 de este texto.

Independiente del texto normativo, en ambos, el principio de transparencia tiene el mismo contenido relativo al deber del responsable de informar al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales. Además, el RGPD señala que se informará sobre los riesgos, la finalidad, las normas, las salvaguardas, la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración; también se informará sobre las modalidades, comunicaciones y notificaciones que permiten el ejercicio de los derechos y la presentación de reclamaciones del titular de los datos, así como de las violaciones de seguridad.

Es evidente, entonces, que se trata de un derecho y un deber de información que no solo ha sido renombrado, sino que se le ha dado un nuevo enfoque debido a que la información no tendría un verdadero valor si es que no cumple con criterios de lealtad, licitud y transparencia. La información por sí sola no es suficiente, puesto que, sin estos adjetivos, presupuestos básicos, no se obtiene el resultado final que es una honesta interrelación entre titulares y responsables.

Pues no debe ser vista como una simple formalidad que se cumplimenta para procesar datos, sino como mecanismo de salvaguarda de los titulares, una verdadera forma de construir una relación entre responsables e interesados basada en el respeto mutuo, ya que permite una eficiente toma de decisiones al titular y, al mismo tiempo, una demostración de la responsabilidad a quien proceda los datos.

[1737] Congreso de la República de Guatemala, *Decreto 57-2008*, 23 de septiembre de 2008, *Ley de Acceso a la Información Pública*, accedido 11 de mayo de 2017, http://www.oas.org/juridico/pdfs/mesicic4_gtm_acceso.pdf.

Además, la transparencia de la información resulta transversal porque gobierna las relaciones entre particulares y autoridades de control en el ámbito de las reclamaciones, entre autoridades de control como parte de un sistema institucional de garantía del derecho y, finalmente, es aplicable a toda información dirigida al público en general, para construir una sociedad que pueda acceder a información y comunicaciones, facilitar el ejercicio de sus derechos subjetivos y contribuir a la generación de una cultura de protección de datos.

En ese sentido, el derecho, deber, principio de información y regla de comunicación de transparencia, lealtad y licitud es la respuesta completa e integral a los actuales desarrollos en el tratamiento de datos personales. Un contenido esencial que se ha ido perfeccionando hasta alcanzar a todos los intervinientes en sus distintas interrelaciones interdependientes, en el sistema de protección de datos personales. Como se ve, se intenta garantizar a los titulares de los datos, mediante toda la información detallada, el ejercicio eficaz de los derechos consagrados, que son parte de un derecho mayor: el derecho a la autodeterminación informativa.

Con esta visión integral que cobija los distintos enfoques antes descritos y del análisis de la normativa europea y de su contraste con la latinoamericana, se puede listar las condiciones, características, tipos de información, entre otras consideraciones que deben conformar la transparencia y que se pasa a analizar a continuación:

a) Características generales

La información para que pueda considerarse transparente, lícita y leal deberá cumplir una serie de características:

i. *Concisa, inteligible y de fácil acceso, con un lenguaje claro y sencillo, de forma gratuita, por escrito, por medios electrónicos o incluso verbalmente,* al tenor de lo que señala el artículo 12 RGPD. En el mismo sentido, el considerando (58) del RGPD señala que cuando la información que se dirija al público en general se requiere que cumpla con las siguientes características: concisa, fácilmente accesible, fácil de entender, utilice un lenguaje claro y sencillo, se visualice, de ser el caso, pueda facilitarse en forma electrónica, si es el caso, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Muchas de estas características coinciden, pero además establecen que cuando la información sea dirigida o afecte a los niños deberá facilitarse en un lenguaje claro y sencillo que sea fácil de entender. En este sentido, que sea un idioma que facilite su entendimiento y comunicación, incluso cuando se trate de contratación electrónica; así lo dispone el artículo 27 de la Ley 34/2002, 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, Publicado en BOE 166, 12 de julio de 2002,[1738] de España.

   Los Estándares Iberoamericanos establecen, además, que la información sea suficiente y fácilmente accesible, especialmente para niñas, niños y adolescentes.

ii. *Previo:* Se refiere a la condición de que la información sea entregada previamente, antes de la obtención del consentimiento. En Latinoamérica, Costa Rica menciona expresamente que debe cumplirse con el deber de información de forma previa, mientras

[1738] *Ley 34/2002*, 11 de julio, *de servicios de la sociedad de la información y de comercio electrónico*, accedido 21 de septiembre de 2018, https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758.

que Argentina, Colombia, Nicaragua, México, Perú, República Dominicana y Uruguay hacen referencia al consentimiento previo e informado. En la normativa española, en su momento, se concibió el deber de información como una obligación previa[1739] porque permitía a los ciudadanos el conocimiento anterior necesario para el ejercicio del principio de consentimiento. Esto porque las condiciones de previo, expreso, preciso e inequívoco van de la mano del consentimiento, pues se consideraban presupuestos necesarios para su validez.

Ahora bien, los Estándares Iberoamericanos, dictados en el 2017 ya no contemplan esta condición de previo. El mismo caso ocurre con el RGPD que tampoco la reconocen, sino que establecen que cuando se obtenga de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información y cuando no se obtenga directamente del interesado, deberá informar con posteridad toda la información prevista en el artículo 4 del RGPD. Como se ve, se deja de lado la condición de previo, porque no se aplica a todos los casos y además porque la condición se sustituye por aquella que solicita que se entregue información en el momento mismo de la recogida cuando se hace directamente del interesado. Y conforme el artículo 4 del RGPD, se señala que el consentimiento del interesado para su validez debe ser "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". Muchas de estas condiciones de validez coinciden con las prescritas en la normativa latinoamericana.

iii. *Sin barreras técnicas:* Que no existan barreras técnicas que impidan su acceso a la información, conforme señala la norma de Colombia, Costa Rica, México, Perú y Uruguay. Es decir que la información pueda ser facilitada independientemente del canal de contacto que se use, ya sea directo a través de la entrevista personal, telefónica, o indirecto, a través de SMS, página web, e-mail; o tal como menciona la ley "cuando se utilicen cuestionarios u otros impresos". Cabe anotar que en todos estos últimos, dicha información deberá figurar inserta en ellos de forma completa y claramente legible. Finalmente, cuando se trate de comunicaciones electrónicas: "Se deberá facilitar información accesible por medios electrónicos sobre los procedimientos de revocación del consentimiento, es decir la forma de darse de baja".[1740]

iv. *Avisos de privacidad*: México y Perú cumplen el deber de información mediante sitios web en los que se difunden los mecanismos y medios disponibles para que el titular manifieste su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular, y puedan consultar el aviso de privacidad simplificado e integral para, de ser el caso, oponerse.

[1739] "En lo que respecta al momento en que una empresa ha de cumplir el deber de información, el apartado 1 del artículo 5 no deja lugar a dudas al exigir que sea «previamente» a la recogida de los datos. Así si ésta se realiza a través de formularios o impresos se puede incorporar a los mismos la cláusula informativa correspondiente de manera que el interesado, antes de proporcionar sus datos, pueda conocer el tratamiento al que serán sometidos. En caso de que los datos se recaben por teléfono o en conversaciones mantenidas con los afectados, antes de iniciar la recogida, ha de informárseles de todas las circunstancias que exige la Ley". SÁNCHEZ MOURIS, "Los datos personales en el inicio de la actividad empresarial", 60.

[1740] C. ALMEIDA y J. MAESTRE, *La Ley de Internet: régimen jurídico de los servicios de la Sociedad de la Información y el comercio electrónico* (España: Editorial Servidoc, 2002), 85.

v. *Documento como medio de prueba:* Documento realizado en cualquier soporte, válido en derecho, que permita ser usado como prueba del cumplimiento de esta obligación. Por ello, "a pesar de que rige el principio de libertad de forma, si la información se proporciona verbalmente, pueden surgir problemas de prueba en un futuro, incumbiendo al responsable del tratamiento acreditar que facilitó toda la información exigida por la Ley [...] Para evitar estos problemas y dejar constancia del cumplimiento del deber de información, aunque no se exige legalmente, se conseja sobre todo a las empresas que canalicen toda la información que les sea posible a través de cuestionarios o impresos y que, para el caso de que exista alguna vía de entrada de información en la que no tengan cabida, incorpore, en la primera comunicación que se efectúe a los titulares de estos datos una cláusula informativa con el contenido preceptuado"[1741]. Aunque esta postura no está recogida en el RGPD, sin embargo para países como Ecuador en los que recién se está comprendiendo el alcance de normativas de protección de datos personales, y ante los escándalos suscitados debido a cobros indebidos por bancos, resulta válida este requisito.[1742] Cabe anotar que la Ley de Defensa del Consumidor, en el artículo 55, prohíbe que se envíe o entregue cualquier servicio o producto al consumidor sin que este lo haya solicitado y obviamente se requiere que exista prueba de esta solicitud.

En ese sentido, la normativa española, por su lado, señala que tanto las comunicaciones previas a la recogida, tratamiento y creación del fichero, como aquellas que, ante una imposibilidad evidente, deban realizarse con posterioridad y que contengan la información que la ley requiere para el cumplimiento del deber de información, ya sea en instrumento independiente o como cláusulas incluidas dentro de una comunicación, carta, –e-mail, contrato, invitación, formulario, impreso de sorteos, etc. deben constar en soporte papel, tal como se colige de la cita anterior, o en soporte electrónico. Además, cuando se haga por vía electrónica, deben estar claramente identificadas como comunicaciones comerciales o incluir la palabra publicidad, según el artículo 20.1 de la LSSI.[1743]

a) Información que debe ser puesta en conocimiento del titular

Los Estándares Iberoamericanos de Protección de Datos Personales, el RGPD y la normativa latinoamericana señalan que el responsable debe facilitar información al titular al menos de los siguientes temas:

i. Sobre el responsable

Tanto la normativa europea como varia de la latinoamericana[1744] determinan que se deberá informar al titular sobre la identidad y los datos de contacto del responsable y, en su caso, de su representante, es decir su dirección de domicilio, teléfonos y correos electrónicos. Sobre domicilio responsable ha legislado Argentina, México, Colombia, Costa Rica, Perú, República Dominicana y Uruguay.

[1741] SÁNCHEZ MOURIS, "Los datos personales en el inicio de la actividad empresarial", 63.
[1742] "GEA Ecuador, otra vez en el ojo de la polémica", accedido 21 de octubre de 2018, https://www.lahora.com.ec/loja/noticia/1102193026/gea-ecuador-otra-vez-en-el-ojo-de-la-polemica.
[1743] *Ley 34/2002*, de 11 de julio, *de servicios de la sociedad de la información y de comercio electrónico*.
[1744] Sobre identidad del responsable legislan Argentina, México, Costa Rica, Perú, República Dominicana y Uruguay.

Esta información puede revestir cierta problemática en el caso de las empresas, ya que "el conocimiento de la identidad y dirección del responsable concreto del tratamiento, no es una cuestión tan obvia como a simple lectura podría derivarse, ya que en ocasiones resulta confuso conocer la identificación de la empresa concreta que va a tratar los datos personales y, por tanto, del responsable del fichero, en grupos empresariales muy integrados, en el uso de Internet —donde convergen diferentes figuras, tales como proveedores de acceso, proveedores de contenido, vendedores a través de correo electrónico, etcétera—. Igualmente el uso de nombres comerciales o marcas pueden confundir a los interesados en el conocimiento de la empresa que efectúa el tratamiento de datos".[1745]

La contactabilidad se refiere a los datos de contacto del responsable puesto que sólo este puede responder ante los derechos ARCO que presente el titular.

2.6.4.2 Sobre el tratamiento

a) *Existencia de la base de datos:* Se deberá informar al titular del dato sobre la existencia misma de la base de datos, archivo, base de datos, electrónico o de cualquier otro tipo y sobre su tratamiento, criterio coincidente en el RGPD y en la normativa de Argentina, Costa Rica, Perú, República Dominicana y Uruguay.

b) *Finalidad de la recogida y del tratamiento:* Otro de los elementos sustanciales que deben ser informados se refiere a la finalidad de la recogida y del tratamiento, tal como señala el RGPD y la normativa de Argentina, México, Colombia, Costa Rica, Nicaragua, Perú, República Dominicana y Uruguay.

c) Es obligación del responsable al momento de cumplir el deber de información y a fin de evitar que el consentimiento sea nulo, que se informe al titular de los datos de la finalidad de forma concisa e inteligible, condiciones generales aplicables a toda entrega de información contemplada en el RGPD. Asimismo, vale la pena aquí citar el artículo 11.3 de la Ley Orgánica de Protección de Datos Personales española que señala además las características de claridad, especificidad e inequívoca de la información relativa a la finalidad, es decir sobre la que se destinarán los datos cuya comunicación está autorizando, así como del tipo de actividad que realiza aquel a quien se pretende comunicar. Todo esto desde la perspectiva de que el titular debe conocer con suficiencia los usos y finalidades a los que sus datos están sometidos.

d) En este mismo sentido, la AEPD respecto de las expresiones "*finalidades promocionales*" y "*de información de productos y servicios*", y de la sentencia de la Audiencia Nacional de 13 de abril de 2005 relativo a la frase "*publicidad comercial*" han señalado que por la amplitud de los términos usados, que son considerados incluso genéricos por las amplias categorías de bienes y servicios que pueden existir en el mercado, no se explicita con una determinación

[1745] ALMUZARA ALMAIDA, "Relaciones precontractuales y contractuales", 89.

suficiente la información que debe ser puesta en conocimiento del afectado para prestar su consentimiento inequívoco, ni tampoco permite al afectado identificar de forma determinada y explícita las finalidades para las que serán tratados sus datos personales en los términos de la LOPD.[1746]

e) De lo que se traduce, que la explicación de la finalidad debe ser profunda y precisa porque no es suficiente apreciaciones generales ya que de esta forma no se cumple con las condiciones analizadas, esto es de claridad, especificidad, inequívoca, ininteligible y concisa.

f) *Motivos de la recogida:* Nicaragua, además, solicita que se expliciten a los titulares los motivos de la recogida y del tratamiento, elemento que valdría la pena rescatar en una normativa en especial cuando los responsables de tratamiento son públicos.

g) *Base jurídica del tratamiento:* Es novedad del RGPD que junto a la finalidad se informe la base jurídica del tratamiento, lo que además de facilitar la comprensión de temas legales permite otorgar seguridad jurídica, tanto en el responsable como en el titular del dato personal. Las categorías de datos personales de que se trate.

h) *Tipos de tratamiento:* El RGPD establece la necesidad de que realice una evaluación de impacto tomando en cuenta el tipo de tratamiento al que se someterán los datos, mientras que en la normativa latinoamericana, específicamente de Colombia, México, Costa Rica, Nicaragua y Uruguay, se considera que los tipos de tratamiento, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, deben ser puestos en conocimiento del titular a fin de que el titular pueda tomar decisiones informadas. Anotándose que en el caso de México esta información podrá estar disponibilizada mediante un aviso de privacidad.

i) *Plazo:* Como parte del tratamiento, es fundamental informar al titular el plazo durante el cual se conservarán los datos personales que deberá coincidir con el de su finalidad; cuando esto no sea posible, deberá informar sobre los criterios utilizados para determinar este plazo conforme dispone el RGPD. Sobre este tema, solo Perú establece un deber de información sobre el tiempo de vigencia de los datos personales en poder del responsable.

j) *Fuentes:* Cuando los datos no han sido obtenidos directamente del titular, el RGPD dispone que deberá informarse la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

k) *Tratamiento ulterior:* Esta precisión tiende a verificar que la actuación de los responsables no se extralimite, en especial cuando el responsable del tratamiento proyecta un tratamiento ulterior de sus datos personales para un fin que no sea aquel para el que se recogieron

[1746] J. Z. DE LA MATA y I. AGÚNDEZ LERÍA, *Protección de datos: comentarios al reglamento* (Lex Nova, 2008), 439.

originalmente, por lo que estará en la obligación de informar al titular sobre otras finalidades y tratamientos ulteriores.

l) *Carácter obligatorio o facultativo de la respuesta:* Existía otra excepción relativa a la obligación de informar sobre el carácter obligatorio o facultativo de la respuesta a las preguntas planteadas y consecuencias de la obtención de datos o de la negativa a suministrarlos recogida por la normativa y la doctrina española[1747] que establecía la necesidad de informar sobre estas condiciones con la finalidad de que el titular pueda tomar una decisión informada y consciente respecto de sus datos. En el artículo 13, numeral 2, literal d) del RGPD se establece que el responsable está obligado a informar si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos. Texto que coincide con lo señalado y contextualiza la necesidad o no de entrega de información debido a una obligación legal o contractual previa que habilita a la recogida y tratamiento de datos.

m) *Confidencialidad:* El responsable deberá informar al titular que los datos personales deban seguir teniendo carácter confidencial porque, por ejemplo, son parte de una obligación de secreto profesional.

n) *Iconos normalizados:* Finalmente, el artículo 12 del RGPD establece otra novedad relativa a posibilidad de entregar la información al titular mediante una combinación con íconos normalizados, que pueden incluso constar en formato electrónico y ser legibles mecánicamente, y que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto.

2.6.4.3 Sobre la cesión

Destinatarios y clases: Se deberá informar a los titulares sobre quiénes pueden ser destinatarios o sobre qué clase de destinatarios pueden consultar sus datos conforme señala el RGPD y la normativa de Argentina, Costa Rica, Perú y Uruguay.

Cesión: El RGPD no señala aspectos relativos a la cesión de datos, sino que la trata de manera genérica como transferencias. Sobre esta temática, la normativa de México, Perú y Uruguay establecen la posibilidad de cesión o transferencia de datos. Ahora bien, el artículo 5.5 de la LOPD española y el artículo 27 del Real Decreto español de 1332/1994, de 20 de junio, por el que se *Desarrollan Determinados Aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*, disponen la obligación del responsable del fichero de que "en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad

[1747] SÁNCHEZ MOURIS, "Los datos personales en el inicio de la actividad empresarial", 63.

del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario". Estas precisiones intentan aclarar que independientemente de quien tenga la base de datos, en este caso un destinatario deberá cumplir el deber de información, anotándose que no solo será necesario, como señala la citada normativa, en la primera cesión, sino en todas aquellas cuando sean necesarias.

Cesión en transferencia internacional de datos: Sobre la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación, o, en el caso de las transferencias mediante garantías adecuadas, normas corporativas vinculantes y a los medios para obtener una copia de estas o al hecho de que se hayan prestado, al tenor de lo indicado en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo del RGPD.

Satisfacción de intereses legítimos: Cuando el tratamiento lícito sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, según lo señalado en el artículo 6, apartado 1, literal f) del RGPD.

Características de claro, concreto y determinado: Deber de informar sobre la finalidad de las cesiones debe ser claro, concreto y determinado, así lo sostiene la Agencia Española de Protección de Datos en la Memoria correspondiente al ejercicio 2001; dice: "Cuando los datos personales recabados a través de Internet vayan a ser comunicados a otras compañías (incluso cuando éstas pertenezcan al mismo grupo empresarial) deberá informarse al usuario, de tal forma que éste pueda conocer explícitamente las finalidades determinadas a las que se destinarán los datos. La información podrá referirse genéricamente a un sector de actividad económica (por ejemplo, servicios financieros [...]), sin que puedan admitirse finalidades indeterminadas o no comprensibles para el usuario (por ejemplo, actividad comercial, actividad publicitaria, empresas del grupo)".

2.6.4.4 Sobre derechos

Derechos de los titulares: Los responsables del tratamiento tendrán la obligación de informar sobre la existencia del derecho a solicitar el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos, cancelación y oposición. En el mismo sentido, solo que limitado a los derechos reconocidos en cada normativa latinoamericana, se informará a los titulares sobre estos derechos y las formas efectivas de ejercerlos en Argentina, Colombia, México, Costa Rica, República Dominicana, Perú y Uruguay.

Por su parte, en la Sentencia de SAN recurso 158/2000, de 15 de junio, se sostiene: "En primer lugar, debe tenerse en cuenta que nos hallamos ante la regulación del

derecho de información a la recogida de datos, derecho importantísimo porque es el que permite llevar a cabo el ejercicio de otros derechos, y así lo valora el texto positivo al pormenorizar su contenido, y establecer la exigencia de que el mismo sea expreso, preciso e inequívoco". Posición semejante se desarrolla en relación al derecho de oposición en los Planes de Oficio 2001 al sector de la Banca Distancia que dicta el Consejo Consultivo la AEPD, que dice: "Deberá también informarse al cliente de los tratamientos que tengan como finalidad la realización de segmentaciones o perfiles de clientes con fines comerciales, así como establecer un procedimiento fácil y directo que permita ejercer la oposición a dicho tratamiento en el momento de la recogida de datos, como por ejemplo la inclusión de una casilla al efecto". Con esto, además de lo señalado en el actual RGPD, se determina mecanismos idóneos, ágiles y eficientes para garantizar el ejercicio de sus derechos al titular.

Datos del delegado de protección de datos: Los responsables deberán informar sobre los datos de contacto del delegado de protección de datos, con la finalidad de direccionar sus reclamos y requerir sus orientaciones específicas en salvaguarda de los derechos como titular.

El derecho a presentar una reclamación ante una autoridad de control.

2.6.4.5 Sobre consentimiento

Revocatoria del consentimiento: Cuando se ha obtenido consentimiento del interesado para el tratamiento de sus datos con fines específicos o para categoría especiales de datos como por ejemplo los sensibles, se informará al titular sobre su derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

Decisiones automatizadas: El responsable del tratamiento informará al titular sobre la existencia de decisiones automatizadas, incluida la elaboración de perfiles, la lógica aplicada, la importancia y las consecuencias previstas de dicho tratamiento, con la finalidad de que el titular pueda hacer uso de sus derechos de oposición o en su defecto de revocatoria del consentimiento, de ser el caso.

Respuestas obligatorias o facultativas y consecuencias: El responsable del tratamiento informará al titular sobre el carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, según lo que señala la normativa de Argentina, Colombia, Costa Rica, Perú y Uruguay. En sentido similar, se informará sobre las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de conformidad con la normativa de Argentina, Costa Rica, Perú y Uruguay.

2.6.4.6 Procedimiento para la entrega de información

El responsable del tratamiento facilitará la información al titular señalada dentro de un plazo razonable de un mes, a menos que por ciertas circunstancias deba ser entregada de forma inmediata en el momento de la obtención de los datos, por ejemplo si se necesita recabar consentimiento.

El responsable del tratamiento facilitará la información al titular, cuando los datos personales se utilicen para comunicación con el interesado, a más tardar en el momento de la primera comunicación.

El responsable del tratamiento facilitará la información al titular, si está previsto comunicarla a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

2.6.4.7 Excepciones al deber de información

Conforme establece el RGPD, se ha establecido un régimen estrictísimo de excepción, que no puede ser aplicado a la ligera por los responsables, ya que está expresamente señalado en la ley y se aplicará cuando los datos personales se hayan obtenido directamente del interesado, pues la única excepción posible es si el interesado ya dispone de la información.

El otro caso expresamente excepcionado en el RGPD es aplicable para cuando la información se haya obtenido directamente del interesado; por la cual el deber de información se exime cuando:

a) El titular ya posea la información.

b) Resulte imposible o suponga un esfuerzo desproporcionado,[1748] tomando en consideración: el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, tomando en cuenta medidas técnicas como la anonimización, seudoanonimización, entre otras reconocidas en el artículo 89, apartado 1 del RGPD.

[1748] Se debe tener cuidado con la afirmación de que resulte imposible o exija esfuerzos desproporcionados, ya que ha ocurrido que como esta excepción debe ser valorada por la autoridad de control, bajo criterios relativos a número de interesados, antigüedad de los datos y posibles medidas compensatorias, el tiempo de respuesta, por ejemplo, de la Agencia de Protección de Datos es demasiado prolongado, por lo que a este respecto autores como Miguel Vizcaíno Calderón señalan que "debido a la necesidad apremiante del responsable consultante de una respuesta inmediata y ante la demora de la AEPD en dictar las resoluciones que faculten a los responsables del fichero a eximirse del deber de información cuando resulte imposible o exija esfuerzos desproporcionados, debe aplicarse la regla del silencio positivo. Es decir, ante el cumplimento del plazo de tres meses sin repuesta, el responsable considera aceptada su petición y por ende no realiza el deber de información". Interpretación que mal usada por las organizaciones podría causar detrimento del derecho a la información que tiene los titulares de los datos.

c) La obtención, registro o la comunicación de los datos personales estén expresamente establecidos por ley.

d) Pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento.

e) Los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional.

f) En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información.

En la normativa latinoamericana no existe un régimen de excepciones expresamente establecido para el deber de información.

De otro lado, el RGPD no toma en cuenta anteriores excepciones como la que establecía que no será necesaria la entrega de información cuando esta se deduzca claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. Excepción que ha sido superada por lo subjetivo de su planteamiento que incluso ha motivado una serie de resoluciones[1749] y que han propiciado su eliminación, más aún cuando es imposible obviar el deber de información respecto de los derechos de acceso, rectificación, cancelación y oposición ya que estos no pueden llegar a deducirse; en consecuencia, volvería en esta parte impracticable e inaplicable esta excepción.[1750]

El artículo 92 de la Constitución y el artículo 49 de la LOGJCC, relativas a la acción de *habeas data*, mencionan que toda persona tendrá derecho a conocer de la existencia, finalidad, origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Si bien esta norma da unas luces, luego de lo analizado, la propuesta normativa para Ecuador debe incluir varios artículos. Esto es un artículo referente a la transparencia como eje rector de los distintos ámbitos de aplicación, al tenor del modelo europeo. Otra norma relativa a las obligaciones del responsable del tratamiento, en el capítulo que corresponda. Otra sobre los derechos de los titulares tanto en lo relativo al tratamiento de la información como de las comunicaciones para el ejercicio de derechos y de reclamaciones por parte de los titulares.

[1749] Una opinión semejante es la que consta en SAN 158/2000, 15 de junio de 2000, que respecto al principio de información en la parte pertinente dice: "La relevancia del derecho conlleva a que su exclusión requiera el mandato expreso de una norma, acogiendo una interpretación estricta, vedándose su extensión mediante artificiosas deducciones. Pues bien, con estas premisas no se aprecia que pueda ser de aplicación el apartado tercero del propio artículo, pues el contenido de la información ni se deduce claramente de la naturaleza de los datos personales que se solicitan [...] así lo considera la Sala, y la parte actora no justifica la claridad de esta deducción; ni de las circunstancias en que se recaban, referidas al momento de prestar consentimiento para efectuar una donación voluntaria de sangre, previa a la inmediata extracción".
Otra sentencia con la que se establece la aplicación restrictiva de esta excepción es la dictada la STSJM, de 17 de mayo de 2002, que considera que "Ese deber de información que, en principio, pesa sobre «Telefónica» en la medida que al contratar la prestación del servicio telefónico recaba —y obtiene— los datos personales del cliente relativos a su nombre, apellidos, dirección, solo quedaría excluido —apartado 3 del art. 5— si el contenido de la información que ha de suministrarse «se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban» y el Tribunal no advierte que del contrato de adhesión que suscribe el cliente de «Telefónica» para la obtención de un servicio de telefonía y de los datos que, para ello, tiene que suministrar se deduzca que «Telefónica tenga un fichero automatizado de datos de carácter personal en el que se van a registrar los datos del cliente, quiénes son los destinatarios de la información de este fichero, el titular del mismo, la existencia de derechos de acceso, cancelación o rectificación»".
[1750] VIZCAÍNO CALDERÓN, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, 107.

Una respecto de la transparencia como principio del tratamiento de los datos personales. Otra acerca del deber de notificación de violaciones de seguridad. Otra respecto de los requisitos necesarios para entregar información al público en general, incluidos la generación de avisos de privacidad limitados o íntegros. Entre todas estas normas incluidas en los distintos capítulos del proyecto normativo, se puede garantizar la transparencia como faro guía de una adecuada entrega de información en el sistema de protección de datos personales.

2.6.4,8 Pertinencia

Tal y como habíamos propuesto en su momento, la necesaria relación que tienen los principios entre sí, invitan a que la efectivización de todos ellos se realice de manera armonizada a fin de garantizarlos en su totalidad, porque la transgresión hacia uno, desestabilizaría a los demás por su indiscutible e intrínseca relación.

Teniendo como precedente lo mencionado, y entrando en plena materia del principio, en los capítulos II y IV, ya se revisó este criterio; así, en el marco de acción del RGPD, el factor pertinencia, recogido en el artículo 5, se ve intrínsecamente aliado con la adecuación y minimización de datos, todos orientados al contexto de la finalidad, las mismas características son las adoptadas por los Estándares de Protección en su precepto 18, bajo el nombre de "Principio de proporcionalidad".

En el contexto de adecuación, Venezuela comparte la apreciación, al recoger en una aproximación al principio de pertinencia, que los datos exigidos deberán ser los estrictamente necesarios. Apuntala al mismo criterio la normativa española, y añade la noción de no excesivos para posteriormente invocar el principio de finalidad; ahora bien, como fue oportunamente revisado, esta finalidad puede resultar un problema en la medida en que al no poder ser determinada al cien por ciento, la franja de vacío se sella con la improbabilidad de evaluar si un dato puede ser adecuado, pertinente y no excesivo. En concordancia con lo expuesto, se determinó que el principio en mención se conjuga de manera determinante con el de finalidad —como también lo determina Uruguay— y obviamente con el de consentimiento, lo que desencadena la obligatoriedad por parte del responsable de obtener la data con criterios de calidad, siendo este contexto también prioritario para Colombia, Argentina, México y Perú. Esto sirve para entender que la pertinencia es parte del principio de calidad de datos y de manera tan elemental que termina por ser consecuente de su objetivo general.

Por otra parte, el considerando 39 del RGPD al referirse a pertinencia, adecuación y minimización de datos señala la implementación de medidas razonables para la rectificación o supresión de los datos personales que sean inexactos como parte de la efectivización de este principio, garantizando además la seguridad y confidencialidad. Por su parte, Paraguay invoca a la exactitud, pero limita su conjugación al ámbito de actualización, determinando a este requisito como base de la pertinencia. Nicaragua, en concordancia, lo implanta en el derecho de cancelación frente al contenido que ha dejado de ser pertinente.

Otro factor aquí adoptado fue la minimización de datos que, aludido en el mismo considerando 39 RGPD, hace referencia al plazo de conservación y, de manera consecuente, al incentivo de trabajar con data seudoanonimizada o mecanismos que permitan a los responsables tratar y usar este tipo datos.

En el mismo marco, el planteamiento de "no excesivo" se distribuye en tres espacios. El primero de ellos ejecutado en relación al ámbito y atendido así en normativa argentina y dominicana; el siguiente, en relación con la finalidad que como ya se había revisado, en el caso puntual, se refiere tanto a la de la recogida como del tratamiento, postura adoptada en países como Argentina, Costa Rica, México, Perú y República Dominicana; finalmente Guatemala lo establece con respecto al propósito de recogida.

Finalmente, las Recomendaciones de la Organización de Estados Americanos sobre Protección de Datos invocan el papel de la pertinencia en el marco de la exactitud. De lo expuesto, es procedente que el principio de pertinencia conste en el artículo relativo a calidad de modo que pueda tener un mayor alcance y se manifieste en todas sus dimensiones.

En este sentido, la normativa propuesta contempla:

> **Artículo 11.- Pertinencia y Minimización de datos personales.-** Los datos personales deben ser pertinentes y limitados a lo mínimo necesario para su finalidad.

2.6.4.9 Calidad

Ecuador alude al presente principio desde el Reglamento del Sistema de Registro de Datos Públicos, cuando señala en el artículo 11, respecto de las condiciones a ejecutar en todo tratamiento de datos personales, bajo el título de Principio de veracidad o calidad de los datos, lo siguiente: "La información contenida [...] debe ser veraz, completa, exacta, actualizada, comprobable y comprensible". En consecuencia, el factor de "veraz" se muestra esencialmente autónomo y principal, como también ocurre en Bolivia.

En particular contexto actúan los Estándares de Protección que señalan entre el catálogo de cualidades del principio en mención a la exactitud, completitud y actualización con miras a la veracidad como objeto; de manera que esta no se muestra como un camino, sino más bien como una finalidad, que además permite añadir constancias respecto de la conservación y la eliminación.

Con respecto al factor veracidad, en conjunto con otros elementos configuran de manera intrínseca este principio. Mientras que en el caso de Argentina, Colombia, Costa Rica, México, Perú, República Dominicana y Uruguay los elementos de mayor realce son los de cierto, veraz o correcto.

El RGPD se aleja aún más de una concepción expresa del principio de calidad, ya que en su lugar se permite orientar a la exactitud —garantizando la rectificación o supresión— y actualización para conseguir este fin. Esta última visión también es adoptada por Paraguay. Y los dos propuestos, por El Salvador, Bolivia y Chile.

Sentado aquello, resulta fundamental revisar brevemente los supuestos que implican el manejo de datos que han dejado de ser actualizados, completos, exactos. Así por ejemplo, en el caso de Argentina se alude directamente a la destrucción, situación que varía sobre la obligatoriedad de ser cancelados en el caso de México y Nicaragua; y por otra parte República Dominicana o Uruguay que consideran eliminarse o suprimirse como propone también el RGPD. Finalmente, Perú invoca al principio de conservación conjugado en relación con la finalidad. No obstante, como en su momento se mencionó, el espíritu mismo

del principio de calidad, bien atendido, resuelve el no tener la necesidad de acudir a estos mecanismos.

Bajo ese supuesto, quien si adopta la fórmula de calidad propiamente es la normativa española en el artículo 4 LOPD, que menciona de forma independiente pero paralela los criterios de pertinencia, adecuación, minimización de datos, finalidad e incompatibilidad; sin embargo, no entrará en una comparación directa porque el mismo artículo les dota de autonomía diferenciándolos, como en su momento ocurrió con Argentina, Costa Rica, México, Perú y República Dominicana que a pesar de incluirse el término dentro de calidad esta relación se niega. El caso más extremo es el de Uruguay y Colombia cuya relación se destruye en su totalidad; lo que no ocurre con Venezuela y Paraguay para los cuales la pertinencia es parte inherente del principio de calidad.

No obstante, previamente nos permitimos concluir que si bien pueden tratarse como dos principios independientes, resulta más eficiente y claro manejar la pertinencia dentro del principio de calidad, con enfoque a la seguridad y permanencia. Pues todos entre todos estos elementos se configura la calidad del dato.

Retomando la perspectiva de la normativa española, se permite contener los presupuestos de exactitud y actualización, como previamente se configuro en la normativa de la Unión Europea, aludiendo a que la participación de estos dos factores se dan a fin de que se refleje la "realidad actual" del titular, por cuanto se manejan tanto en su recogida como en su posterior tratamiento, en donde la obligación de dar aviso al responsable sobre cualquier cambio que se presente este sobre los hombros del titular para que paso seguido, ejerza su derecho a la rectificación y demás mecanismos que serán de obligatoria implementación por parte del responsable. En este contexto, aliado directo de estos criterios, es el deber de información conjugado con campañas de actualización de datos, y demás canales de comunicación y puntos de contacto que faciliten el cometido.

Chile, Argentina, Costa Rica, México, Perú, República Dominicana y Uruguay varían toda consideración hasta el momento tratada, puesto que tratan la calidad como parte del principio de finalidad, al igual que El Salvador para el que, en lugar de tratarse de un principio pertenece a las obligaciones de los entes públicos.

Para El Salvador, Bolivia y Chile los elementos que configuran el principio de calidad, son: exactos, actualizados, veraces, completos, precisos, verificables e inteligibles. Mientras que Argentina, Costa Rica, Perú, República Dominicana incluyen el término adecuado; Uruguay el de ecuánime; Costa Rica, Perú, República Dominicana, Guatemala, Colombia y Uruguay, el de exacto; Argentina, Costa Rica y Colombia el de completo; Argentina, México, Perú y República Dominicana el de actualizado; mientras que el de comprobable y comprensible lo incluye Colombia; y el de necesario, Perú. Respecto de no ser excesivo en relación al ámbito, Argentina y República Dominicana; o en cuanto al propósito de recogida, Guatemala.

Finalmente, las Recomendaciones de la Organización de Estados Americanos sobre Protección de Datos Personales contenido se refieren a lo que la doctrina y legislación específica denominan principio de calidad, por el cual se establece una obligación de cuidado y verificación de la actualización, completitud, corrección y exactitud de la información personal recopilada.

Finalmente, el principio de calidad de los datos es como dice el Tribunal Supremo "uno de los ejes fundamentales de la regulación del tratamiento automatizado de datos personales y exige que los datos deben ser exactos, adecuados, pertinentes y proporcionados a los fines para los que han sido recogidos y tratados".[1751]

De lo dicho la normativa que recoja el principio de pertinencia y el de calidad de los datos personales es el siguiente:

> **Artículo 15.- Calidad.-** Los datos personales que sean objeto de tratamiento deben ser exactos; íntegros; precisos; completos; comprobables; claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad.
>
> La Autoridad de Protección de Datos Personales definirá los casos en los cuales se deberán actualizar los datos personales y su periodicidad.

2.6.4.10 Finalidad

El principio de finalidad es uno de los primeros reconocidos a escala internacional para la protección de los datos personales del titular. El RGPD y los Estándares Iberoamericanos de Protección de Datos y los Principios establecidos por la OEA, también lo desarrollan. En tal sentido, dicho principio establece que los datos personales serán recogidos con fines legítimos y lícitos, y por medios justos y legales;[1752] además es condición indispensable que sean fines determinados y explícitos. Finalmente, debe verificarse que el tratamiento es coherente o responde a la finalidad señalada, y por tanto es adecuado, pertinente y limitado, y, de no ser así, la prohibición de tratamiento en estos casos y cuando las finalidades son distintas a las autorizadas. Los medios justos y legales hacen referencia a que la recopilación debe ser compatible con los requisitos jurídicos pertinentes y con las expectativas razonables, esto es que no pueden ser obtenidos mediante fraude, engaño o pretextos falsos.[1753]

De ese modo, será el responsable del tratamiento el que defina las finalidades de la obtención, registro y tratamiento de una base de datos, la cual será revisada por una autoridad de control para verificar el cumplimiento de las condiciones necesarias para un adecuado tratamiento.

Cabe destacar que el principio de finalidad se encuentra directamente relacionado con el deber de información y, por ende, el principio de transparencia, ya que las características relativas a la legitimidad, licitud, explícita y determinada finalidad para la cual se trataran datos deberán ser puestas en conocimiento de los interesados en el momento de la recogida, con lo cual se cumple el deber de información transparente y leal.

Asimismo, gracias a que se determinan los fines del tratamiento por parte de un responsable, se puede establecer cuando los datos personales son adecuados, pertinentes y limitados en su uso y, por tanto, necesarios para los fines para los que sean tratados, con un plazo de

---

[1751] Sala Primera del Tribunal Supremo español, "Sentencia 672-2014" de TS, Sala 1.ª de lo Civil, 19 de noviembre de 2014, vLex, accedido 19 de octubre de 2018, https://supremo.vlex.es/vid/551912746.

[1752] Asamblea General OEA, 86 Período Ordinario de Sesiones, CJI/doc. 474/15 rev.2 Río de Janeiro, Brasil, 26 marzo 2015, *Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales*, http://www.oas.org/es/sla/ddi/docs/cji-doc_474-15_rev2.pdf.

[1753] Ibíd.

conservación mínimo estricto que no supere aquel que permita la consecución de los fines especificados,[1754] e identificado aquellos casos en los que deben tratarse pues no pueden lograrse razonablemente por otros medios. Todo ello desde la perspectiva de que las finalidades y el tratamiento sean éticos, congruentes y respetuosos con las personas.

Ahora bien, se puede tratar datos con fines distintos de aquellos para los que fueron recogidos los datos inicialmente, siempre y cuando sean compatibles con los fines de su recogida inicial, o concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación, o se trate de datos históricos, para archivo general, investigación científica y estadística o, en su defecto, se haya autorizado por el titular en el momento de la obtención del consentimiento.

Por su parte, el principio de finalidad en Latinoamérica es de los pocos que se encuentra presente en todas las normativas analizadas,[1755] ya sea que su reconocimiento sea constitucional o legal.

Sobre las características que desarrolla el principio de finalidad, se tiene similar criterio que lo dispuesto en la normativa europea: que sean finalidades lícitas y legítimas en salvaguarda de los titulares del dato personal, tal como consta en la normativa de Argentina, Colombia, México, Uruguay y Costa Rica.

Adicionalmente, tal como ocurre en Europa, países latinoamericanos entre los que destaca Uruguay, establecen que la finalidad está directamente relacionada con la obligación del responsable de determinar la finalidad del tratamiento y el deber de informar sobre este al titular del dato;[1756] por tanto, un derecho de este de exigir que se le informe en tal sentido,[1757] con la supervigilancia que una autoridad de control puede realizar sobre la coherencia. No obstante, Argentina, México, Costa Rica y Uruguay mencionan el término compatibilidad, entre lo informado al interesado y la evidencia del tratamiento mismo que se esté dando a tales datos. Todo esto determina que este procesamiento es legítimo y lícito, no solo en el momento de la definición de la finalidad misma, sino durante su tratamiento, así como en su uso. Cabe anotar que si esta compatibilidad no existe, se requiere de nuevo consentimiento del titular, o en su caso, la eliminación de los datos de quien no autorice y la disponibilidad de que los titulares puedan exigir sus derechos.

Otras características propias del sistema latinoamericano son: la de explicitar las finalidades en la cesión de datos,[1758] la utilización de acciones constitucionales como el *habeas data* para conocer la finalidad de un tratamiento[1759] y del uso de los datos, el bloqueo,[1760] la

[1754] Asamblea General de Naciones Unidas, http://200.33.14.21:83/20121122060127-12869.pdf, 9.
[1755] Argentina, Colombia, Costa Rica, Ecuador, Guatemala, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay.
[1756] Argentina, Colombia, Guatemala, México, Nicaragua, Perú, República Dominicana y Uruguay establecen la obligación de informar sobre la finalidad de la recolección, uso, tratamiento e incluso de la cesión de los datos personales.
[1757] Argentina, Nicaragua, República Dominicana, Costa Rica y Ecuador conciben que es derecho de los titulares recibir información respecto de la finalidad de la recolección, uso, tratamiento y cesión de los datos personales.
[1758] Argentina, México, Nicaragua y Uruguay.
[1759] Argentina, Nicaragua, Guatemala (únicamente bases de datos de responsables públicos) y Uruguay. Ecuador también debería utilizar desde esta perspectiva, pero lamentablemente no existe aplicaciones en este sentido.
[1760] México y Nicaragua.

actualización, la cancelación y la eliminación[1761] por haberse agotado la finalidad para la cual fue recabado el dato o suscitarse incompatibilidades o incoherencias posteriores.

Ahora bien, la Resolución 45/95 de la Asamblea General, 14 de diciembre de 1990,[1762] establece además que es necesario incorporar en las legislaciones lo relativo a la imposibilidad de levantar la confidencialidad para fines incompatibles y sin autorización del titular y la mención sobre la temporalidad de la permanencia de los datos en relación con sus fines.

En el caso del Ecuador, la normativa constitucional en el apartado relativo al derecho constitucional (numeral 19 del artículo 66 de la CRE) no incluye la definición ni el alcance del principio de finalidad. Sin embargo, el artículo 92 de la CRE determina que las personas tendrán derecho a conocer el uso y la finalidad de sus datos personales. En este sentido, la acción constitucional del *habeas data* tiene entre uno de sus objetivos el facilitar al interesado el conocer la finalidad de la recogida, el tratamiento y el uso de datos personales, con lo cual se puede revisar además la pertinencia, la licitud y la legitimidad de las actuaciones del responsable. En normativa de mucho menor nivel, consta en el artículo 11 del Reglamento a la Ley del Sistema Nacional de Registro de Datos Públicos lo respecto al principio de finalidad como uno de los aplicables en el intercambio de información entre instituciones públicas para garantía de un tratamiento adecuado, en el caso de responsables públicos.

De lo señalado se concluye que en una propuesta normativa debe contemplarse a la finalidad como principio que debe reflejar la licitud, legitimidad del tratamiento, para lo cual el responsable deberá determinar de forma explícita las finalidades para las cuales realizará la obtención, tratamiento y uso de la información. De modo que mediante este principio se pueda garantizar un uso adecuado, pertinente y limitado en cuanto a tiempo de conservación. Asimismo, va de la mano del principio de transparencia por el cual se deberá informar al titular sobre las finalidades y con ello se permite el control posterior de las actuaciones del responsable como mecanismo de garantía de un tratamiento adecuado.

Se deben incluir las características propias establecidos en la normativa latinoamericana como la posibilidad de que los titulares puedan reclamar ante una autoridad de control un tratamiento apartado de las finalidades informadas al titular o de finalidades ilegítimas o ilícitas, lo que faculte bloqueos o eliminaciones, de ser el caso.

El numeral 17 de los estándares determina el principio de finalidad por el cual todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas. El responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquellas que motivaron el tratamiento original de estos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación. Es decir, los elementos sustanciales son la identificación de finalidades determinadas, explícitas y legítimas, y la prohibición de tratamiento para finalidades distintas a las autorizadas.

Finalmente, es destacable el precepto por el cual no se considerará incompatible con las finalidades iniciales y se faculta el tratamiento ulterior de datos personales con fines

[1761] México, Costa Rica y Uruguay.
[1762] Asamblea General de Naciones Unidas, http://200.33.14.21:83/20121122060127-12869.pdf.

archivísticos, de investigación científica e histórica o con fines estadísticos, en favor del interés público. Este contenido no consta en la normativa latinoamericana vigente.

> **Artículo 10.- Finalidad.-** Las finalidades del tratamiento deberán ser determinadas, explícitas y legítimas, no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme el principio de legitimidad.

2.6.4.11 Seguridad adecuada al riesgo

La normativa europea y latinoamericana concibe a la seguridad como un principio fundamental de la protección de datos personales. Debido a los avances tecnológicos, el modelo inicial de protección asociada a medidas de seguridad por niveles y naturaleza de los datos,[1763] ha tenido que ser superado por nuevas formas de afrontar las brechas y riesgos que, además, deben reflejar una responsabilidad proactiva y demostrada[1764] del responsable y encargado del tratamiento.

El RGPD y la normativa latinoamericana[1765] establecen un sistema organizado, estratificado, estructurado e integral que permite detectar desviaciones, intencionales o no, de información y para garantizar, conforme señala el Estándar Iberoamericano de protección de Datos personales, la confidencialidad, integridad y disponibilidad de los datos personales y la seguridad adecuada, que incluye la protección contra el acceso, uso, tratamiento, transmisión, transferencia, consulta, conservación no autorizada o ilícita o fraudulenta, la adulteración, o alteración accidental o ilícita, pérdida, destrucción, daño[1766] o daño accidental, o la revelación o divulgación,[1767] o la contaminación mediante virus informáticos,[1768] mediante la aplicación de medidas técnicas u organizativas apropiadas.

Para la implementación de un nivel de seguridad adecuado al riesgo el responsable y el encargado del tratamiento deben:

a) evaluar los riesgos inherentes al tratamiento;[1769]

[1763] España, *Ley Orgánica 15/1999*, 13 de diciembre, d*e Protección de Datos de Carácter Personal*, 13 de diciembre de 1999, BOE núm. 298, 14 de diciembre de 1999, pp. 43088 a 43099.

[1764] Agencia Española de Protección de Datos, Agencia Catalana de Protección de Datos y Agencia Vasca de Protección de Datos, *Guía del Reglamento General de Protección de Datos para responsables de tratamiento*, accedido 14 de octubre de 2018, https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf.

[1765] Argentina, Colombia, Costa Rica, Ecuador, Guatemala, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay.

[1766] El RGPD en el considerando (85) señala como daños producidos por violaciones a la seguridad de los datos personales a la pérdida de control sobre sus datos personales, restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional o cualquier otro perjuicio económico o social significativo para la persona.

[1767] Asamblea General OEA, 86 Período Ordinario de Sesiones, CJI/doc. 474/15 rev.2 Río de Janeiro, Brasil, 26 marzo 2015, *Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales*, http://www.oas.org/es/sla/ddi/docs/cji-doc_474-15_rev2.pdf .

[1768] Asamblea General de Naciones Unidas, http://200.33.14.21:83/20121122060127-12869.pdf.

[1769] Para lo cual deberán tomar en cuenta, conforme señala el RGPD: el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, los riesgos de probabilidad que

b) aplicar medidas para mitigar el riesgo;[1770]

c) aplicar medidas técnicas y organizativas apropiadas,[1771] otras normativas latinoamericanas incluidos los Estándares Iberoamericanos de Protección de Datos personales determinan; además, la necesidad de medidas administrativas como: Argentina, Colombia, México, Nicaragua, Perú, República Dominicana y Uruguay. Colombia incluye medidas humanas tendientes a evitar brechas de seguridad provocadas por acciones de personas físicas. Asimismo, México, Nicaragua y Costa Rica hablan de medidas físicas relativas a la infraestructura de los espacios en los cuales se recaba o tratan datos. Finalmente, Costa Rica habla de medios lógicos y Perú de medios legales; este último resulta interesante puesto que obliga a diseñar medidas en este ámbito y además las vuelve de aplicación general y obligatoria;

d) aplicar un proceso periódico de establecimiento, implementación, operación, monitoreo, revisión, mantenimiento, mejora continua,[1772] verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas implementadas para garantizar la seguridad del tratamiento;[1773]

e) aplicación de un formato y procedimientos para la notificación de violaciones de la seguridad de los datos personales,[1774]}

f) notificación a la autoridad de control de una violación de seguridad de los datos personales;

g) notificación del encargado del tratamiento al responsable de tratamiento de una violación de seguridad de los datos personales;

h) notificación al interesado cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para sus derechos y libertades para permitirle tomar las precauciones necesarias;

i) no será necesaria la comunicación si el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas que haga ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el

---

presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. También la gravedad de las variables para los derechos y libertades de las personas físicas o la naturaleza de los datos personales que deban protegerse en especial datos sensibles. Asimismo, tal como determinan los Estándares Iberoamericanos: las transferencias internacionales de datos personales que se realicen o pretendan realizar, el número de titulares; las posibles consecuencias que se derivarían de una vulneración para los titulares; las vulneraciones previas ocurridas en el tratamiento de datos personales.

[1770] Por ejemplo: La seudonimización, el cifrado de datos personales.

[1771] Por ejemplo: La capacidad de garantizar confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico, entre otros.

[1772] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.

[1773] La adhesión a un código de conducta o a un mecanismo de certificación aprobado podrá servir para demostrar el cumplimiento de la aplicación de medidas técnicas y organizativas.

[1774] Sin dilación indebida, en un tiempo razonable, cumpliendo disposición de autoridades de control, entre ellas las autoridades policiales.

cifrado o que garanticen que ya no exista la probabilidad de que se concrete el alto riesgo para los derechos y libertades del interesado, o suponga un esfuerzo desproporcionado y optará en su lugar por una comunicación pública o una medida semejante;

j) documentar cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.

k) prohibición de registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad, en concordancia con lo planteado por Argentina, Costa Rica, República Dominicana y Uruguay.

Respecto de las citadas notificaciones, el RGPD en el artículo 33 y los Estándares Iberoamericanos de Protección de Datos Personales determinan el contenido mínimo de la notificación sobre violaciones de seguridad de los datos personales ya sea a los interesados, a la autoridad de control o del encargado al responsable:

e) Describir la naturaleza de la violación de la seguridad de los datos personales, como las categorías y el número aproximado de interesados y registros afectados.

f) Comunicar el nombre y datos de contacto del delegado de protección de datos o de un contacto que pueda entregar más información.

g) Describir posibles consecuencias de la violación de la seguridad.

h) Describir medidas correctivas adoptadas o propuestas por el responsable y, si proceden, medidas adoptadas para mitigar los posibles efectos negativos.

i) Las recomendaciones al titular sobre las medidas que este pueda adoptar para proteger sus intereses.[1775]

j) Los medios disponibles al titular para obtener mayor información al respecto.[1776]

El Ecuador por su parte contempla una visión muy limitada de seguridad porque el texto de la Constitución vigente propone la aplicación de medidas de seguridad únicamente para datos sensibles. Al tenor del artículo 92 de la CRE sobre la acción de *habeas data* que señala que: "En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias".

De otro lado, el artículo 21 del Reglamento a la Ley de Comercio Electrónico considera datos sensibles del consumidor "sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de

[1775] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1776] Ibíd.

los cuales puedan cometerse fraudes o ilícitos que le afecten",[1777] por lo que desde esta interpretación solo estos datos ameritan medidas de seguridad.

En el mismo sentido, los datos reservados relativos a niños, niñas y adolescentes, en especial aquellos relativos antecedentes penales[1778] también son de carácter sensible y al tenor de la norma ecuatoriana ameritan protección.

La Ley de Seguridad Pública y del Estado establece la prohibición expresa de obtener información, producir inteligencia o almacenar datos sobre personas por el solo hecho de su etnia, orientación sexual, credo religioso, acciones privadas, posición política o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción.[1779]

La Ley del Sistema Nacional de Registro de Datos Públicos respecto de datos sensibles, que utilizados en el ámbito del intercambio de información entre instituciones públicas, delegadas o que brindan servicios públicos, establece que deben contar con un sistema de protección especial: confidencialidad y altos niveles de seguridad para proteger y garantizar la reserva de la información que reposa en sus archivos. El acceso a estos datos solo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el/la titular de la información pueda ejercer.[1780]

De otro lado, la Ley de Telecomunicaciones, artículo 85, determina que la Agencia de Regulación y Control de las Telecomunicaciones establecerá y reglamentará los mecanismos para supervisar el cumplimiento de las obligaciones, para garantizar tanto el secreto como la seguridad de las comunicaciones y la protección de datos personales.

En suma, en Ecuador la seguridad como principio tiene visión sesgada y sectorial, pues es solo aplicable por vía residual a ámbitos relativos al intercambio de información entre públicos, en el ámbito de la seguridad nacional, de los ficheros cuyo responsable es el Estado, incluso desde el ámbito patrimonial y de servicios de comercio electrónico como de telecomunicaciones. Lo que sin duda no representa un sistema integral de seguridad, pues que deja por fuera al sector privado y a otros ámbitos públicos; además no contempla definiciones básicas sobre el alcance y aplicación de medidas técnicas, organizativas para la implementación de la seguridad.

> **Artículo 46.- Seguridad de datos personales.-** El responsable o encargado del tratamiento de datos personales, según sea el caso, deberá sujetarse al principio de

[1777] Presidencia de la República del Ecuador, *Reglamento a la Ley de Comercio Electrónico. DEJ 3496*, Registro Oficial 735, 31 de diciembre de 2002. Lexis Ecuador, accedido 22 de noviembre de 2017, www.silec.com.ec.
[1778] Congreso Nacional del Ecuador, *Código de la Niñez y Adolescencia. Ley 100*. Registro Oficial 737, 3 de enero de 2003. Lexis Ecuador, accedido 2 de junio de 2017, www.lexis.com.ec.
[1779] Asamblea Nacional del Ecuador, *Ley de Seguridad Pública y del Estado. Ley 0*, Registro Oficial Suplemento 35, 28 de septiembre de 2009., Lexis Ecuador, accedido 22 de noviembre de 2017, www.silec.com.ec.
[1780] Asamblea Nacional Ecuador, *Ley 0, Ley del Sistema Nacional de Registro de Datos Públicos*, Registro Oficial Suplemento 162, 31 de marzo de 2010. Última modificación: 12 de septiembre de 2014. Lexis Ecuador, 31 de marzo de 2010, www.silec.com.ec.

seguridad de datos personales, conforme lo dispuesto en el artículo 17 de la presente Ley Orgánica; para lo cual deberá tomar en cuenta el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos y el nivel de impacto que estos representen a los derechos fundamentales y libertades individuales.

El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales.

El responsable o encargado del tratamiento de datos personales deberá demostrar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados. Entre otras medidas, se podrán incluir las siguientes:

Medidas de anonimización, encriptación, cifrado o codificación de datos personales;

Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y,

Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, organizativa, y jurídica.

Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares para medición y gestión de riesgos, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales.

Artículo 51.- Notificación de vulneración de seguridad.- El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales, dentro del término de 3 días después de tener conocimiento de ella.

El encargado de tratamiento deberá notificar al responsable la vulneración de la seguridad de datos personales en un plazo no mayor a 2 días después de tener conocimiento de ella.

En caso de retraso del responsable o del encargado del tratamiento de datos personales en la notificación de vulneración de seguridad, sin que intermedie la debida justificación, se aplicarán las sanciones correspondientes, conforme a lo establecido en la presente Ley.

En la notificación deberá constar lo siguiente:

a) La descripción de la naturaleza de la vulneración de la seguridad de los datos personales;

b) Las categorías y el número aproximado de titulares afectados;

c) Las categorías y el número aproximado de registros o campos de datos personales afectados;

d) El nombre y los datos de contacto del delegado de protección de datos, o a falta de este, de cualquier otro punto de contacto; }

e) La descripción de las posibles consecuencias de la vulneración de la seguridad de los datos personales;

f) La descripción de las medidas adoptadas, implementadas o propuestas por el responsable para remediar la vulneración de la seguridad de los datos personales; y,

g) De ser el caso, las medidas adoptadas e implementadas para mitigar los posibles efectos negativos de la vulneración de la seguridad de datos personales.

Una vez tomado conocimiento de la vulneración de las seguridades de datos personales, el responsable deberá efectuar el análisis de riesgo sobre los derechos de libertad de sus titulares.

La notificación de las vulneraciones de seguridad de datos personales tendrá como objeto principal que la Autoridad de Protección de Datos Personales lleve un registro estadístico sobre vulneraciones e identificar posibles medidas de seguridad para cada una de ellas, así como identificar sectores o instituciones más vulnerables y promover nuevas regulaciones que busquen mejorar las seguridades exigibles a los responsables de tratamiento y otorgar seguridad jurídica en el tratamiento de datos personales.

La Autoridad de Protección de Datos Personales sólo podrá sancionar al responsable o encargado del tratamiento, cuando la vulneración de seguridad de datos personales ha sido producto de incumplimientos a las medidas de seguridad adecuadas. En tal caso, la notificación oportuna de la violación por parte del responsable de tratamiento, tanto a la autoridad como al titular, así como las medidas de respuesta adoptadas, serán considerados como un atenuante de la infracción.

En caso de no cumplimiento del término para la notificación, el responsable del tratamiento deberá proceder a justificar la dilación, caso contrario, se procederá conforme al régimen sancionatorio establecido para el efecto.

2.6.4.12 Consentimiento

El consentimiento es el principio que permite al titular de los datos, ejercer el derecho a la autodeterminación informativa, pues faculta al titular a controlar su datos y decidir qué, a quiénes, en qué condiciones, qué finalidades y por cuánto tiempo se entregarán los datos personales que le conciernen.

Conforme el RGPD, el Estándar Iberoamericano de Protección de Datos Personales y la normativa latinoamericana el concepto de consentimiento es el de toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta y autoriza el tratamiento de datos personales de su titularidad. Es la manifestación de voluntad libre de vicios que acepta de forma informada sobre la recogida y tratamiento de sus datos personales.

En ese sentido, los principales elementos que constituyen un consentimiento válido que produce efectos jurídicos son:

a) *Declaración o clara acción afirmativa:* El consentimiento podrá ser otorgado ya sea mediante una declaración o una clara acción afirmativa, actos que servirán para que el responsable demuestre de manera indubitable que el titular otorgó el citado consentimiento. El RGPD supera una vieja discusión sobre si es aceptable el consentimiento tácito, aquel que se deriva de la inactividad, silencio o falta de oposición del afectado ya no es procedente, descartándolo completamente, puesto que como se señaló previamente se requiere una acción afirmativa, es decir una exteriorización de la voluntad, mediante una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal, como la de hacer clic en una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o "*cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta*".

   Se puede utilizar un consentimiento inequívoco de forma implícita cuando se deduzca de una acción del interesado, puesto que de esta manera no resulta en una inacción como ocurría con el consentimiento tácito, sino que se entiende que existe una acción implícita como la de continuar navegando por una web y aceptar que se utilicen cookies para monitorear su navegación.

b) **Todas las actividades y fines del tratamiento:** El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines y para cada uno de ellos. De tal forma, que se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales, en garantía del elemento sustancial del consentimiento conocido como libertad.

c) **Revocatoria del consentimiento:** El consentimiento podrá revocarse en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos, y no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Por su parte, varios países latinoamericanos como Argentina, Costa Rica, México, Nicaragua, Perú y Uruguay señalan que respecto de la cesión el consentimiento es revocable. Mientras que México y Perú señalan que la revocabilidad puede producirse en cualquier momento. Perú y Costa Rica requieren que la revocatoria cumpla con los mismos requisitos o de la misma forma en que se obtuvo la autorización, a decir por escrito o cualquier medio equivalente. Nicaragua y México si se cumple con los criterios constantes en el aviso de privacidad.

d) **Consecuencias del consentimiento:** El consentimiento, además, es el elemento fáctico que faculta al responsable a captar, tratar y ceder datos personales y deberá ser capaz de demostrar que cuenta con tal consentimiento. Por ello, Uruguay señala que el consentimiento expreso deberá documentarse.

e) **Libre:** Obtenido sin vicios del consentimiento, sin error, fuerza o dolo, "no debe existir riesgo de engaño intimidación o coacción, este debe ser apropiado para la edad y la capacidad de la persona", porque de no cumplirse el consentimiento sería inválido y no

facultaría la recogida, tratamiento e inclusión en una base de datos. Aclarándose que el consentimiento no podrá constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal cuando exista un desequilibro o estado de desventaja y se encuentra forzado directa o indirectamente a ceder sobre su autodeterminación informativa, como cuando el responsable es autoridad pública, o empresa; esto debido a que resulta probable que el consentimiento no se haya dado libremente, que la necesidad de acceder a bienes o servicios y beneficios sociales (considerando [43], RGPD), o cuando el interesado no goza de verdadera o libre elección pues no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno. Por su parte, de los países latinoamericanos solo Argentina y Nicaragua recogen el criterio de libertad del consentimiento.

f) **Específico:** El titular debe conocer y consentir de forma específica, definida, determinada o concreta la operación, el tratamiento y las finalidades explícitas sobre todo respecto de datos sensibles, decisiones individuales automatizadas, incluida la elaboración de perfiles; flujo trasfronterizo de datos personales. De la recolección de sus datos y de su inclusión en una base de datos, no caben interpretaciones extensivas o analógicas, ya que no sería procedente establecer un consentimiento continuado para futuros tratamientos ni para una cesión indefinida. Por su parte, México, Nicaragua, Panamá, República Dominicana y Uruguay usan el criterio "consciente", mientras que Costa Rica usa el término "preciso", pero en suma cualquiera de estos avoca a la necesidad de explicitar el consentimiento.

g) **Informado:** Para otorgar un consentimiento libre de vicios, debe cumplirse con el principio de información, ya que solo de esta manera se garantiza la ausencia de error; por ende que el titular conozca, comprenda y, en consecuencia, decida sobre el tratamiento, uso y cesión de sus datos personales. Como se analizó en la transparencia y deber de información, ya no es necesario que la información sea previa a la recogida del consentimiento, pero países como Colombia, Costa Rica, México, Perú, República Dominicana y Uruguay determinan la necesidad de que el consentimiento se obtenga mediante una información clara y completa en el que se le advierta de las consecuencias de la entrega de sus datos. Por su parte, los principios de la OEA señalan que sin claridad, el consentimiento no es válido, pues este debe basarse en suficiente información.

h) **Explícito:** Consiste en la característica del consentimiento por el cual el titular de forma expresa y explícita, exterioriza su voluntad inequívoca, esto es que no genere dudas sobre su emisión ni sobre su intención. Es decir, que no cabe duda de la manifestación de voluntad conforme señala la normativa de Costa Rica, Nicaragua, Perú y Uruguay. Se requiere de consentimiento inequívoco y explícito para el tratamiento de datos sensibles, la adopción de decisiones automatizadas y las transferencias internacionales.

Por su parte, Argentina, Colombia, Costa Rica, Guatemala, México, Perú, República Dominicana y Uruguay señalan que además el consentimiento debe ser expreso. Solo Argentina y República Dominicana señalan que el consentimiento deberá figurar en forma expresa y destacada. Mientras que Nicaragua usa el término inequívoco para suplir la característica de expreso.

i) **El momento de la recogida del consentimiento:** La discusión de si el consentimiento debe ser previo al tratamiento ha sido superada y no existe limitación temporal en su recogida pudiéndose realizar antes, durante o después de este. Excepto cuando se necesite consentimiento expreso, como el caso de los datos sensibles.

j) **Modelos de declaración de consentimiento:** La respectiva autoridad deberá proporcionar un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas que contenga como mínimo la identidad del responsable del tratamiento, las actividades y los fines del tratamiento de los datos personales.

k) **Consentimiento de niños:** El RGPD determina que deberán tener 16 años los adolescentes a quienes se les oferte directamente bienes o servicios de la sociedad de la información. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

l) **Consentimiento realizado por representantes legales o apoderados:** Si bien son los titulares por esencia los que otorgan consentimiento; sin embargo, Costa Rica y Nicaragua además facultan expresamente también a los representantes legales o apoderados.

m) **Consentimiento para la Cesión:** Mientras que el RGPD no menciona a la cesión de forma específica, sino que se atribuyen a esta acción todo el régimen de protección constante en la norma; sin embargo, en varios países latinoamericanos como Argentina, Nicaragua, México, República Dominicana y Uruguay requieren que exista consentimiento previo del titular para la cesión; de modo que el titular conozca sobre la finalidad de la transferencia y la identificación del cesionario. Solo México requiere que el titular pueda manifestar su negativa para el tratamiento y que Nicaragua y República Dominicana faculten cesiones si están directamente relacionados con el interés legítimo del cedente y del cesionario.

En la normativa ecuatoriana, la Constitución en el artículo 66, numeral 19, dispone únicamente que puedan tratarse datos de existir consentimiento o mandato legal; en este sentido es en la normativa de orden legal donde deben definirse las condiciones y cualidades del consentimiento como mecanismo de resguardo de la protección de los datos de las personas. De otro lado, en norma de carácter sectorial que regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, por medio de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas (art. 1, Ley de comercio electrónico, firmas electrónicas y mensajes de datos) se establece que el consentimiento debe ser expreso, sin que se haya definido el alcance y contenido de esta expresión.

De lo analizado, se colige que debe constar en una normativa para Ecuador un artículo que recoja todos los elementos analizados y que, en consecuencia, se recoja también en el articulado relativo a las definiciones; además se establezcan las condiciones de su ejercicio en normativa posterior.

Artículo 13.- Consentimiento.- Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular de hacerlo.

El consentimiento será válido, cuando la manifestación de la voluntad sea: libre, es decir, que se encuentre exenta de vicios del consentimiento; especificidad, se refiere a la determinación concreta de los medios y fines del tratamiento; informada, aquella que cumple con el principio de transparencia y efectiviza el derecho a la transparencia; inequívoca, que no se presenten dudas sobre el alcance de la autorización otorgada por el titular; previa, que

el consentimiento se haya dado con anterioridad al tratamiento, ya sea en el momento mismo de la recogida del dato cuando se obtiene directamente del titular y excepcionalmente de forma posterior cuando los datos personales no se obtuvieren de forma directa; expresa, que de manera indubitable el responsable pueda demostrar que el titular manifestó su voluntad a través de una declaración o acción clara, afirmativa o se deduzca de una acción del titular.

El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento igual de sencillo que el que fue llevado para recabar el consentimiento.

El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos.

> **Artículo 35.- Consentimiento relativo a categorías especiales de datos.-** Además de los requisitos del consentimiento previstos en el artículo 13, se requiere de la manifestación de la voluntad explícita del titular para el tratamiento de datos sensibles, datos crediticios y de datos personales de adolescentes mayores a 16 y menores de 18 años.
>
> Para el caso de adolescentes mayores a 12 y menores de 16 años, así como de niñas y niños es necesario contar con el consentimiento explícito y verificable de su representante legal. La Autoridad de Protección de Datos Personales definirá los parámetros de verificación del consentimiento.
>
> Se entiende por consentimiento explícito aquel que puede ser demostrado de manera indubitable por el responsable o encargado del tratamiento de datos personales, en relación a la autorización otorgada por el titular a través de una declaración o acción clara y afirmativa.
>
> El responsable o encargado del tratamiento de datos personales está en obligación de verificar si el titular o representante legal ha otorgado su consentimiento explícito para el tratamiento de datos sensibles, datos crediticios y en especial, datos de niñas, niños y adolescentes.

2.6.4.13 Otros principios

La normativa latinoamericana y la europea han previsto otros principios, además de los tradicionales aplicables a la protección de datos personales, debido a que cada realidad plantea la necesidad de atender o fortalecer determinados temas, como por ejemplo:

a) *Principio de cesión:* Argentina permite la cesión de datos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario, solicitando para ello consentimiento informado del titular de los datos. Este principio se relaciona con el de finalidad y con el de consentimiento y precisa la situación de la cesión que bajo la perspectiva de este país amerita una protección específica. El RGPD no hace mención a la cesión o transferencia, sino exclusivamente cuando se habla de intercambio de datos con terceros países, porque entiende que esta actividad se rige bajo los mismos criterios que el tratamiento y que no existe necesidad de un régimen diferente.

b) *Principio de integridad:* Colombia señala que este principio prohíbe un manejo de datos incompleto, pues tal situación puede distorsionar la veracidad de la información. En realidad este principio es parte del de calidad de la información, pero este país considera necesario relevarlo por sí mismo y darle la categoría autonómica de principio debido a que su Corte considera necesario ordenar al responsable completar la información y evitar transgresiones de derechos sobre todo en el ámbito financiero.

c) *Principio de disposición:* Perú señala que todo titular debe contar con vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos y, a diferencia del RGPD, establece como principio lo que en este instrumento consta como derecho a la tutela judicial efectiva.

d) *Principio de nivel de protección adecuado:* Perú consagra como principio la necesidad de un nivel suficiente de protección, conforme estándares internacionales en la materia, para los datos personales que se vayan a tratar fuera del país. Nuevamente, en este país esta temática tiene importancia relevante por lo que la normativa le otorga el rango de principio.

e) *Principio de lealtad:* República Dominicana considera necesario este principio para prohibir recoger los datos por medios fraudulentos, desleales o ilícitos. Por su parte, los Estándares Iberoamericanos señalan que por el principio de lealtad además el responsable debe abstenerse de tratar datos a través de medios engañosos o fraudulentos, y que son desleales aquellos tratamientos de datos personales que den lugar a una discriminación injusta o arbitraria contra los titulares.[1781] Este principio es parte del de legalidad como en el caso del Perú y del principio de calidad como el caso del Uruguay y Argentina. Uruguay lo denomina *principio de veracidad pero añade que*, además de no permitirse la recogida por medios desleales, fraudulentos, tampoco se lo puede hacer por medios abusivos o extorsivos. Mientras que la OEA lo llama *principio relativo a propósitos legítimos y justos*, por el cual señala que los datos personales deben de ser recopilados solamente para fines legítimos y por medios justos y legales, por lo que los datos no pueden ser obtenidos mediante fraude, engaño o pretextos falsos.[1782]

f) *Principio de no discriminación:* La ONU señala entre uno de los principios el de no discriminación, por el cual no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias; así como la circunstancia de ser miembro de una asociación o sindicato. Al respecto, se considera que en lugar de un principio esta debe ser una prohibición que admita excepciones amparadas en las diferentes necesidades legítimas de crear bases con estos contenidos sensibles precisamente para que los Estados puedan cumplir con sus misiones como atención a grupos vulnerables.[1783]

Realizado el análisis respectivo, se considera que no es necesario incluir los citados principios, sino que sus contenidos deben completar los ya existentes con la finalidad de mejorarlos y hacerlos más precisos e integrales.

[1781] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1782] Asamblea General OEA, 86 Período Ordinario de Sesiones, CJI/doc. 474/15 rev.2 Río de Janeiro, Brasil, 26 marzo 2015, *Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales*, http://www.oas.org/es/sla/ddi/docs/cji-doc_474-15_rev2.pdf.
[1783] Asamblea General de Naciones Unidas, http://200.33.14.21:83/20121122060127-12869.pdf, 95.

A continuación se desarrollarán los principios que si se debe incluir en una normativa para Ecuador, toda vez que presentan nuevas formas de protección que deben aplicarse y con ello adecuarse a los avances de la ciencia y la tecnología.

2.6.4.13.1 Principio de proporcionalidad

Este principio se encuentra recogido en el Estándares Iberoamericanos de Protección de Datos Personales, en el RGP, en alguna legislación latinoamericana y en jurisprudencia por lo que debe ser entendido desde varias perspectivas:

a) *Proporcionalidad y ponderación de derechos:* El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe ponderarse frente a otros derechos fundamentales, en particular el respeto a la vida privada y familiar, del domicilio y de las comunicaciones, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, a la diversidad cultural, religiosa y lingüística, el libre desarrollo de la personalidad.

b) *Nivel equivalente de protección:* Garantizar un nivel equivalente entre la protección de las personas físicas y la libre circulación de datos; es decir, respeto por la dignidad humana, al mismo tiempo que se permita el desarrollo económico, social y cultural que brindan los avances tecnológicos.

c) *Proporcionalidad en la licitud del tratamiento:* El RGPD establece que cuando el tratamiento no esté basado en el consentimiento del interesado o en la ley y se pretenda tratar para otro fin distinto de aquel para el que se recogió, se debe ponderar para verificar que dicho tratamiento es necesario y proporcional en una sociedad democrática para salvaguardar la seguridad y defensa del Estado o la seguridad pública, para lo cual se deberán tomar en cuenta varias condiciones expresamente detalladas en la ley.

   De la normativa latinoamericana, solo Perú reconoce a la proporcionalidad cuando determina que todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados. Los estándares además sostienen que deben ser pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento. La OEA sostiene que la proporcionalidad impone limitaciones generales al uso de dichos datos. En realidad, estos últimos criterios son parte de los contenidos del principio de finalidad, de calidad y pertinencia de los datos personales.

d) *En el tratamiento de categorías especiales de datos personales:* Desde la perspectiva que los datos sensibles están prohibidos de tratar a menos que el tratamiento sea necesario por razones de un interés público esencial, establecido en la ley y proporcional entre el objetivo perseguido y el respeto a la protección de datos personales, para lo cual se deben establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

e) *Proporcionalidad en las sanciones:* Otro de los espacios donde es necesario aplicar la proporcionalidad es en el de las sanciones por infracciones cometidas por responsables o

encargados, conforme la sentencia del Tribunal de Justicia de la Unión Europea en el caso Lindqvist, emitida el 6 de noviembre de 2003.

Se propone el siguiente texto normativo:

> **Artículo 12.- Proporcionalidad del tratamiento.-** El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo en relación a las finalidades para las cuales han sido recogidos o a la naturaleza de las categorías especiales de datos.

2.6.4.13.2 Principio de legitimación

Únicamente los Estándares Iberoamericanos de Protección de Datos Personales conciben el principio de legitimación, desde la perspectiva de que es la ley la que autoriza el tratamiento de datos personales, y es el propio legislador, en el momento de elaboración de esta, el que realizó un análisis de ponderación entre el respeto a la protección de los datos personales y el flujo de información que permite el desarrollo económico, político, social y cultural para determinar aquellos casos en que esta autorización se justificaba y que en general se refieren a: el consentimiento para una o varias finalidades específicas; el cumplimiento de una orden judicial, resolución o mandato motivado de autoridad pública competente; el ejercicio de facultades propias de las autoridades públicas o se realice en virtud de una disposición legal; el reconocimiento o defensa de los derechos del titular ante una autoridad; necesario para la ejecución de un contrato o precontrato en el que el titular sea parte; necesario para el cumplimiento de una obligación legal aplicable al responsable; necesario para proteger intereses vitales del titular o de otra persona física; necesario por razones de interés público previstas en la ley; necesario para la satisfacción de intereses legítimos del responsable o de un tercero. Pero estos intereses no podrán prevalecer por sobre los intereses, los derechos o libertades fundamentales del titular, en particular de niños, niñas o adolescentes, por ser estos de atención prioritaria. Este análisis no será aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus competencias. Constituye de interés legítimo el tratamiento de datos personales de contacto imprescindibles para la localización de personas físicas a los que el responsable presta sus servicios.

Respecto de este principio, su relación con el principio de licitud es innegable por lo que es preferible agruparlo e incorporarlo en una sola normativa que se denomine principio de legitimación y licitud, porque una vez realizado el análisis de legitimidad, las causas y casos de tratamiento están autorizados legalmente como se verá a continuación.

2.6.4.13.3 Principio de licitud

El RGPD y los Estándares Iberoamericanos de Protección de Datos personales, una parte de la normativa latinoamericana, así como las Recomendaciones de la ONU y de la OEA incluyen el principio de licitud como aquel que determina que todo tratamiento de datos personales debe ser lícito y leal.

Por tanto, es la ley la que autoriza a los responsables el tratamiento o no de datos personales, en virtud de un análisis de legitimación de cada caso supuesto, tal como se analizó en el principio de legitimidad.

El RGPD establece las condiciones que debe cumplir el tratamiento para considerarse lícito, entre los cuales está el consentimiento del interesado, la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento, la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato, el cumplimiento de una obligación legal, la protección de intereses vitales, interés público o ejercicio de poderes públicos, satisfacción de intereses legítimos. Sobre las condiciones de aplicabilidad de cada uno de estos supuestos, el RGPD hace un análisis pormenorizado. En el caso de la normativa ecuatoriana, la norma debe ser de carácter general, que incluya los criterios señalados previamente en el principio de legitimación, para que todo lo relativo al ámbito, alcance, requisitos, condiciones y restricciones se establezca mediante reglamentos.

Por su parte, Argentina, Perú y Uruguay, así como las Directrices para la regulación de los archivos de datos personales informatizados (Resolución 45/95 de la Asamblea General de las Naciones Unidas, 14 de diciembre de 1990, y en el Proyecto de Ley Modelo sobre Protección de Datos Personales, tomando en cuenta los estándares internacionales alcanzados en la materia. AG/RES. 2842 [XLIV-O/14]) reconocen el principio de licitud. Este principio no solo aplica a la autorización para el tratamiento, sino a que el responsable tratará los datos personales con estricto apego a las normas legales, el derecho internacional y los derechos y libertades de las personas.

Argentina y Uruguay conciben también dentro del principio de licitud que las bases de datos no tengan finalidades contrarias a las leyes o a la moral pública. Uruguay añade que las bases de datos no pueden tener finalidades violatorias de derechos humanos.

Por su parte, las Recomendaciones de la OEA señalan al principio de legalidad y lealtad como aquel por el cual "la información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales, ni debe ser utilizada para fines contrarios a los fines y principios de la Carta de Naciones Unidas". Esta definición se apega más a los principios de finalidad y al de lealtad.

Se concluye, entonces, que el principio de licitud permite que el legislador prevea en el momento de elaboración de las leyes los casos o situaciones que justifican un tratamiento de datos, un régimen diferenciado ya sea maximizando o limitando las reglas de protección con ponderación, legitimidad y justicia, por medio de reserva de ley.

Artículo 9.- Legitimidad.- El tratamiento solo será legítimo y lícito si se cumple con alguna de las siguientes condiciones:

a) Exista obligación en el ordenamiento jurídico aplicable al responsable del tratamiento;

b) Por orden judicial, resolución o mandato motivado de autoridad pública competente;

c) Para el ejercicio de las competencias y facultades establecidas en la Constitución, la Ley, tratados internacionales ratificados por el Ecuador y demás normativa aplicable a favor de las entidades pertenecientes al sector público, sus delegatarios y organizaciones de Derecho Internacional Público;

d) Para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado;

e) Para la ejecución de medidas precontractuales a petición del titular, excepto cuando prevalezcan los intereses o los derechos y libertades de niñas, niños y adolescentes como titulares;

f) Por consentimiento del titular para el tratamiento de sus datos personales para una o varias finalidades específicas; o,

g) Para proteger intereses vitales, del interesado o de otra persona natural, como por ejemplo su vida, salud o integridad.

2.6.4.13.4 Principio de responsabilidad proactiva y demostrada

Este principio de reciente incorporación es reconocido en el RGPD y establece que el responsable de tratamiento debe cumplir con los deberes impuestos por la ley para garantizar un tratamiento lícito y adecuado de los datos personales bajo su dominio, así como desarrollar innovaciones, emprendimientos mientras se respetan los derechos humanos. Todo ello desde una perspectiva proactiva o diligencia debida; en otras palabras, debe realizar actividades más allá de las dispuestas en la norma, pero que se deducen de ella,[1784] por ser de su deber mínimo de cuidado, como por ejemplo documentar e identificar claramente la base legal sobre la que se desarrollan los tratamientos. Además, debe ser demostrada, esto es que pueda probarse que se han implementado las acciones que se le increpan, y que sirve precisamente para probar la intencionalidad de cumplir y su buena fe,[1785] no solo desde la perspectiva de la lista de obligaciones que se derivan de las actuaciones propias que se presentan el momento de realizar una recogida, procesamiento, comunicación o difusión de la información, sino también desde un enfoque sobre el ciclo de existencia, usabilidad y destrucción del dato personal.

Asimismo, conforme señalan los Estándares Iberoamericanos de Protección de Datos Personales, el responsable y el encargado deberán adoptar e implementar medidas correspondientes para el cumplimiento de los principios de protección[1786] y revisar y evaluar de manera periódica y permanente los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones, así como rendir cuentas sobre el tratamiento de datos personales a la autoridad de control.[1787]

La Asamblea General de las Naciones Unidas determina que, con el objetivo de respetar y proteger el derecho a la privacidad, en virtud del derecho internacional de los derechos humanos, incluso en el contexto de las comunicaciones digitales, los Estado deben adoptar medidas, procedimientos, prácticas y legislación, para poner fin a las violaciones de esos derechos y creen las condiciones necesarias para impedirlas; en especial en lo relativo a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales,

[1784] Agencia Española de Protección de Datos, Agencia Catalana de Protección de Datos, y Agencia Vasca de Protección de Datos, *Guía del Reglamento General de Protección de Datos para responsables de tratamiento*.
[1785] Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, artículo 30.
[1786] Asamblea General OEA, 86 Período Ordinario de Sesiones, CJI/doc. 474/15 rev.2 Río de Janeiro, Brasil, 26 marzo 2015, *Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales*, http://www.oas.org/es/sla/ddi/docs/cji-doc_474-15_rev2.pdf.
[1787] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.

incluidas las realizadas a gran escala.[1788] Si bien este supuesto no es referente directo de la responsabilidad proactiva y demostrada; sin duda este es un principio que contribuye directamente a cumplir con las Recomendaciones de Naciones Unidas.

Por su parte, solo Uruguay concibe a la responsabilidad como principio, pero su contenido es completamente diferente pues hace alusión a la responsabilidad civil, administrativa y penal del responsable del tratamiento en el caso de incumplimiento de las obligaciones señaladas.

Situaciones de vulnerabilidad

El RGPD determina las situaciones de vulnerabilidad que determinan mayores niveles de cuidado y por tanto de responsabilidad:

a) casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales;
b) datos sensibles: que revelan el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas;
c) crear o utilizar perfiles personales, para los cuales se evalúan aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos;
d) datos personales de personas vulnerables, en particular niños;
e) tratamiento de una gran cantidad de datos personales y afecte a un gran número de interesados.

Condiciones generales

a) Cuando dos o más responsables determinen los objetivos y los medios del tratamiento, serán considerados corresponsables del tratamiento, a menos que de modo transparente y de mutuo acuerdo consten sus respectivas responsabilidades, funciones y relaciones en el cumplimiento de las obligaciones.
b) Son corresponsables también y en particular en cuanto al ejercicio de los derechos del interesado y del deber de información.
c) Son corresponsables en la designación un punto de contacto para los interesados y en la puesta en conocimiento de los interesados de los aspectos esenciales del acuerdo.
d) Los responsables aun cuando exista un acuerdo podrán ejercer sus derechos frente a, y en contra de, cada uno de los responsables art. 26, RGPD).
e) El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite (art. 31, RGPD).
f) Tanto el encargado del tratamiento como cualquier persona que actúe bajo la autoridad del responsable o del encargado solo podrá tratar datos personales bajo las instrucciones del responsable, a no ser que estén obligados a ello en virtud una norma expresa (art. 29, RGPD).

[1788] Asamblea General de las Naciones Unidas, *Resolución A/C.3/68/L.45/Rev.1 sobre el Derecho a la Privacidad en la Era Digital*, accedido 26 de mayo de 2018, http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1&referer=http://www.protecciondedatos.org.mx/2013/12/resolucin-naciones-unidas-derecho-privacidad-digital/&Lang=S.

g) Si un encargado del tratamiento infringe la normativa al determinar los fines y medios del tratamiento, se presume que es responsable del tratamiento (art. 28, RGPD).

Obligaciones

m) Cumplir con los criterios de aplicación general, los contenidos de cada uno de los principio de tratamiento que constan en la respectiva norma y con el ámbito, alcance y aplicabilidad de los derechos de los titulares.

n) La responsabilidad requiere se realice una atribución clara de las obligaciones.

o) Es obligación del responsable elegir para el tratamiento de datos personales, únicamente, al encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas (art. 27, RGPD).

p) El encargado del tratamiento no podrá recurrir a otro encargado sin que medie autorización previa por escrito, específica o general, por parte del responsable que le ha designado.[1789]

q) Establecer un contrato u otro acto jurídico entre responsable y encargado que, conforme la ley vigente, tendrá entre su contenido mínimo el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Además, dicho contrato o acto jurídico estipulará de forma expresa que el encargado debe tratar datos personales a dirección escrita del responsable, regulará la transferencia de datos personales a un tercer país o una organización internacional, respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria, las medidas de seguridad necesarias. Respetar las formalidades para elección de otros encargados que ofrezcan garantías suficientes.

r) El encargado deberá asistir al responsable, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para responder a las solicitudes de ejercicio de los derechos de los interesados.

s) Ayudar al responsable a garantizar el cumplimiento de las obligaciones de seguridad, de notificación de una violación de la seguridad a la autoridad de control y al interesado; realizar, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento que de resultar pertinente habilitará a realizar una consulta previa ante organismo de control y vigilancia.

t) Suprimir o devolver todos los datos personales, a petición del responsable, una vez finalizada la prestación de los servicios de tratamiento, y suprimir las copias existentes a menos que se requiera la conservación de los datos personales de conformidad con la ley.

u) Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, y para permitir la realización de auditorías,

[1789] De producirse algún cambio en la incorporación o sustitución de otros encargados, se informará al responsable, dándole así la oportunidad de oponerse. Si el encargado recurre a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico válido, las mismas condiciones previstas entre el encargado original y el responsable, en particular aquellas relativas a la prestación de garantías suficientes de medidas técnicas y organizativas. Si ese otro encargado incumple sus obligaciones, el encargado inicial seguirá siendo plenamente responsable (art. 27, RGPD).

inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable. El encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el RGPD.

Responsabilidades de los responsables y encargados de tratamiento

Desde la perspectiva de la responsabilidad y la seguridad como principio, el RGPD y la normativa mexicana, señalan varias obligaciones que deben cumplir el responsable y el encargado del tratamiento, es decir por él mismo o por su cuenta, o por otros o terceros en su nombre, o por su orden o disposición, y que son las siguientes:

a) Implementar medidas oportunas y eficaces, que observen la naturaleza, ámbito, contexto y fines del tratamiento, y que analizando el riesgo para los derechos y libertades de las personas físicas lo eviten (considerando [74], RGPD).

b) Implementar mecanismos demostrables respecto de las medidas impuestas que cumplan con la normativa, incluida su eficacia (considerando [74], RGPD).

c) Elaborar y revisar periódicamente políticas y programas de protección de datos personales obligatorios, y hacerlos obligatorios[1790] y exigibles al interior de la organización.[1791]

d) Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.[1792]

e) Destinar recursos autorizados para la instrumentación de programas y políticas.[1793]

f) Diseñar, desarrollar e implementar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente ley y las demás que resulten aplicables en la materia.[1794]

g) Medidas técnicas y organizativas apropiadas, como las de adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto (considerando [78], RGPD).

h) Reducir al máximo el tratamiento de datos personales (considerando [78], RGPD).

i) Seudonimizar lo antes posible los datos personales (considerando [78], RGPD).

[1790] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1791] Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en posesión de sujetos obligados*.
[1792] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1793] Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en posesión de sujetos obligados*.
[1794] Ibíd.

j) Transparentar las funciones y el tratamiento de datos personales (considerando [78], RGPD).

k) Facultar a los interesados supervisar el tratamiento de datos (considerando [78], RGPD).

l) Crear y mejorar elementos de seguridad (considerando [78], RGPD).

m) Implementar privacidad por diseño y por defecto al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios, programas, sistemas o plataformas informáticas, aplicaciones electrónicas, productos o cualquier otra tecnología que impliquen un tratamiento de datos personales, [1795] incluidos los contratos públicos que están basados en el tratamiento o que tratan datos personales para cumplir su función (considerando [78], RGPD). Para lo cual el responsable del tratamiento o el encargado aplicará medidas preventivas de diversa naturaleza que permitan emplear de forma efectiva los principios, derechos y demás obligaciones previstas:[1796] 1) Medidas desde el diseño, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, así como medidas técnicas y organizativas apropiadas como: a) Seudonimización, tomando en cuenta que debe implementarse lo antes posible; b) Reducir al máximo el tratamiento de datos personales, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de estos, sin la intervención del titular, a un número indeterminado de personas,[1797] minimización de datos; c) Dar transparencia a las funciones y l tratamiento de datos personales; d) Permitir a los interesados supervisar el tratamiento de datos; e) Permitir al responsable del tratamiento crear y mejorar elementos de seguridad; f) Los principios de la protección de datos desde el diseño y, por defecto, también deben tenerse en cuenta en el contexto de los contratos públicos. 2) Medidas por defecto: Deberán aplicarse medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento: a) los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento; b) que no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas; c) se aplique a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

n) Mantener registros de las actividades de tratamiento bajo su responsabilidad (considerando [82], RGPD).

o) Cooperar con la autoridad de control y a poner a su disposición, previa solicitud, los citados registros, de modo que puedan servir para supervisar las operaciones de tratamiento (considerando [82], RGPD).

[1795] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1796] Ibíd.
[1797] Ibíd.

p) Poner en práctica un programa de capacitación y actualización.[1798] Por su parte, El Salvador establece la obligación de capacitar periódicamente a todos sus servidores públicos en materia del derecho de acceso a la información pública y el ejercicio del derecho a la protección de datos personales.

q) Incluir en planes de estudio de educación formal para los niveles inicial, parvulario, básico y medio, contenidos que versen sobre la importancia democratizadora de la transparencia, el derecho de acceso a la información pública, el derecho a la participación ciudadana para la toma de decisiones y el control de la gestión pública y el derecho a la protección de datos personales, conforme señala la normativa de El Salvador.

r) Establecer un sistema de supervisión y vigilancia[1799] interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.[1800]

s) Establecer procedimientos para recibir y responder dudas y quejas[1801] de los titulares.[1802]

t) Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.[1803]

u) Establecimiento y designación de un representante de los intereses del titular del dato y/o evaluador de las actividades del tratamiento en organismos públicos o privados.

v) Realizar evaluaciones de impacto, mecanismo previo y proactivo por el responsable y encargado desde sus respectivas responsabilidades, en conjunto y en colaboración, deben verificar los tratamientos antes de que se produzca cuando estos pudieran causar particular gravedad, sean del alto riesgo, o tengan probabilidad de causar perjuicio a sus titulares para lo cual se establecerán criterios orientadores.[1804] El Estado realizará evaluaciones de impacto generales

[1798] Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en posesión de sujetos obligados*.
[1799] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1800] Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en posesión de sujetos obligados*.
[1801] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1802] Cámara de Diputados del H. Congreso de la Unión de Estados Unidos Mexicanos, *Ley General de Protección de Datos Personales en posesión de sujetos obligados*.
[1803] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1804] Según el RGPD, se entiende como tales cuando: a) se van a utilizar nuevas tecnologías; b) la naturaleza, alcance, contexto o fines, entrañen un alto riesgo para los derechos y libertades de las personas físicas; c) se va a realizar una evaluación sistemática y exhaustiva de aspectos personales de personas físicas, que se realizan mediante un tratamiento automatizado, mediante la elaboración de perfiles, o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas, cuyas decisiones pueden tener efectos jurídicos o afecten significativamente respecto de personas físicas concretas; d) se va a realizar un tratamiento a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales; e) se van a realizar operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados, porque por ejemplo porque hacen más difícil para los interesados el ejercicio de sus derechos; f) se va realizar una observación sistemática a gran escala para el control de una zona de acceso público, en particular cuando se utilicen dispositivos optoelectrónicos; g) para cualquier otro tipo de operación cuando la autoridad de control competente considere

para cada base jurídica, pero cuando una actividad específica cumpla los criterios de riesgo se necesitará una evaluación de impacto específica a menos que esta haya sido evaluada cuando se realizó la evaluación de impacto general. Se debe discutir si el procedimiento para realizar una evaluación de impacto y su correspondiente informe debe estar a nivel de ley o de reglamento.[1805]

w) Realizar consulta previa a la autoridad de control, para determinar las mejores acciones para un tratamiento que en la evaluación de impacto haya tenido respuesta negativa, antes de iniciar las actividades de tratamiento, en especial cuando entrañen un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación.

x) Establecer medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales toma en cuenta los resultados de la evaluación de impacto.

y) Designar un delegado u oficial de protección de datos personales o figura equivalente, conforme el artículo 37 del RGPD, y artículos 37, 38 y 39 de los Estándares Iberoamericanos de Protección de Datos —que se analizarán a continuación— cuando concurran una de las siguientes circunstancias: a) el tratamiento lo realice una autoridad pública; b) lleven a cabo tratamientos de datos personales y sensibles que tengan por objeto una observación habitual y sistemática de la conducta del titular; c) realicen tratamientos de datos personales que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, considerando las categorías de datos personales tratados, como datos sensibles; las transferencias que se efectúen; el número de titulares; el alcance del tratamiento; las tecnologías de información utilizadas o las finalidades de estos, entre otras.

Dichas normativas, señala además, que de oficio y aunque no se encuentre en una de las causas previstas, el responsable podrá designar a un oficial de protección de datos personales si así lo estima conveniente.[1806] El delegado tendrá independencia y no recibirá instrucciones por parte del responsable ni del encargado.[1807] El responsable estará obligado a respaldar al oficial de protección de datos personales en el desempeño de sus funciones, facilitándole los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de estos.[1808]

El oficial de protección de datos personales tendrá, al menos, las funciones siguientes: a) Asesorar al responsable respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales, en especial sobre la evaluación de impacto y la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes; b) Coordinar, al

---

que el tratamiento entrañe probablemente un alto riesgo para los derechos y libertades de los interesados, en particular porque: impida a los interesados ejercer un derecho, utilizar un servicio, ejecutar un contrato, porque se efectúe sistemáticamente a gran escala. No debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o clientes, un solo médico, otro profesional de la salud o abogado (considerando [91], RGPD.

[1805] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.

[1806] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.

[1807] Ibíd.

[1808] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.

interior de la organización del responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la ley;[1809] c) Supervisar al interior de la organización del responsable el cumplimiento de la normativa; d) actuar como punto de contacto con la autoridad de control para consultas previas y otras consultas, y colaborar con ella.[1810]

Mecanismos de demostración

Como parte de los mecanismos[1811] a los cuales los sujetos pasivos pueden acogerse para demostrar una actuación diligente y, por ende, responsable que evite la imposición de sanciones o su atenuación, constan los siguientes:

a. Códigos de conducta o códigos tipo aprobados,[1812] que son aquellas normas que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de la regulación de la actuación de responsables y encargados del tratamiento en el cumplimiento de los deberes, derechos y principios de la protección de datos personales, atendiendo el riesgo probable que se derive del tratamiento para los derechos y libertades de las personas físicas, en especial debido a las cuestiones particulares de cada sector especializado y sus características propias y específicas respecto del tratamiento y de las necesidades específicas de las microempresas y las pequeñas y medianas empresas, según el considerando (98) y el artículo 40 del RGPD. Argentina en su normativa, señala además que estos esquemas de autorregulación deberán contener mecanismos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas eficaces en caso de incumplimiento.

   Por su parte, Costa rica señala que para que sean válidos los protocolos de actuación, deberán ser inscritos —así como sus posteriores modificaciones— ante el organismo de control, como también dispone el RGPD. Sobre la elaboración, la modificación, ampliación, adhesión por parte de responsables y encargados a códigos de conductas, se desarrollará en un reglamento los aspectos relacionados para el efecto por parte de la autoridad de control. Respecto de los contenidos mínimos que deben tener los códigos de conducta, por ser fundamental para establecer un adecuado nivel de protección, deben tratarse a nivel legal, ya sea que posteriormente puedan ser mejorados o perfeccionados en una normativa reglamentaria. Los elementos mínimos que deben constar en un código de conducta son la determinación de: el tratamiento leal y transparente, los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos, la recogida de datos personales, la seudonimización de datos personales, la información proporcionada al público y a los interesados, el ejercicio de los derechos de los interesados, la información proporcionada a los niños y la protección de estos. Así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño, las medidas y procedimientos de responsable del tratamiento, las medidas y

[1809] Ibíd.
[1810] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.
[1811] Aquellos por los cuales, las autoridades de protección pueden proporcionar directrices, que previo análisis del riesgo relacionado con el tratamiento, determinen directrices que el responsable o el encargado del tratamiento deben cumplir y que le permiten a posterior demostrar el cumplimiento o la identificación de buenas prácticas para mitigar el riesgo (considerando [77], RGPD).
[1812] Argentina determina que las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante, por lo que estos códigos de conducta pueden acogerse por varios actores dentro del sistema de protección de datos personales.

procedimientos para aplicar la privacidad por diseño y por defecto, las medidas y procedimientos para garantizar la seguridad del tratamiento, la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados, la transferencia de datos personales a terceros países u organizaciones internacionales, los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos, los procedimientos para presentar una reclamación ante una autoridad de control —conforme el artículo 77 del RGPD—, los procedimientos para presentar acciones judiciales ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento, tutela judicial efectiva (art. 79, RGPD). Por su lado, Costa Rica requiere que se describan los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales. En la normativa latinoamericana únicamente Argentina, Uruguay, México y República Dominicana reconocen a los códigos de conducta.

b. Esquemas de autorregulación[1813] pero, como se señala en los otros mecanismos, estos deben ser aprobados.

c. Certificaciones aprobadas,[1814] o cualquier otro mecanismo, con el objeto de medir su nivel de eficacia,[1815] como sellos de confianza.[1816] Sobre los requisitos, procedimientos para la aprobación de organismos dedicados a emitir o revocar certificaciones constará en un reglamento que para el efecto dicte la autoridad de control.

d. Directrices dadas por una autoridad de control.

e. Indicaciones proporcionadas por un delegado de protección de datos.

f. La autoridad de control también puede emitir directrices sobre operaciones de tratamiento que no supongan un alto riesgo para los derechos y libertades de las personas físicas, e indicar qué medidas pueden ser suficientes en dichos casos para afrontar el riesgo en cuestión.

g. Estándares.[1817]

h. Mejores prácticas nacionales o internacionales.[1818]

[1813] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1814] Se entiende por certificaciones, sellos y marcas de protección de datos personales, aquellos mecanismos voluntarios que responsables, encargados pueden acoger, principalmente respecto de trasferencias a terceros países u organizaciones internacionales, o aquellos que sean vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, por los cuales se puede aumentar la transparencia y el cumplimiento de la normativa de protección, incluidas las relativas a los derechos de los interesados respecto de las operaciones de tratamiento, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes (considerando [100], RGPD) y demostrar el cumplimiento de lo dispuesto en el RGPD por parte de responsables y encargados, tomando en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas, según lo dispuesto en el artículo 42 del RGPD.
[1815] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1816] Ibíd.
[1817] Ibíd.
[1818] Ibíd.

La normativa latinoamericana,[1819] excepto Perú, Colombia y México (normativa aplicable solo a sujetos obligados públicos), las Recomendaciones de la ONU y de la OEA, así como los Estándares Iberoamericanos de Protección de Datos Personales (aunque existe un artículo que específica obligaciones específicas del encargado de tratamiento) no establecen una lista de obligaciones o deberes que los responsables o encargados del tratamiento deben cumplir, ya que se ha optado por un sistema en el que se proponen una serie de criterios generales, principios del tratamiento que deben ser cumplidos y de derechos que deben ser respetados por todos los intervinientes en el tratamiento de datos, eso incluye titulares, responsables y órganos de control. Cabe resaltar que para los responsables y encargados de tratamiento estos criterios generales, principios y derechos se entienden obligaciones que deben ser cumplidas; caso de no serlo, debe considerarse una infracción que amerita la sanción correspondiente.

Pese a este señalamiento, el RGPD establece una serie de acciones y mecanismos que deben ser cumplidos por el responsable y el encargado con miras a establecer un sistema de responsabilidad activo que involucra una actitud proactiva y positiva, como un intento de que la protección se vuelva real. Los entornos tecnológicos son dinámicos y de evolución constante por lo que todos los días existen retos que deben ser asumidos por los responsables, pues no existen protocolos, ni reglas, ni normas, ni conocimientos estáticos que permitan formas lineales o tradicionales de protección, sino que, por el contrario, no todo está escrito y cada día aparecen nuevas formas de aplicar lo conocido, inventos o avances que deben ser entendidos y dimensionados, de modo que involucran mediciones de riesgos, análisis de las realidades tecnológicas y sociales para prever o al menos intentar hacerlo si los usos y aplicaciones de estas tecnologías pueden generar daños a los derechos y libertades individuales.

De lo anotado, es necesario que la normativa ecuatoriana distinga claramente entre los deberes de responsables y tratamientos asociados a los principios, como mínimos de cumplimiento del tratamiento de datos y las otras responsabilidades asociadas al principio de responsabilidad proactiva y demostrada. Además de una necesaria claridad en el tema, es indispensable para la determinación de infracciones y, por ende, del régimen de sanciones que permite la vigencia de una ley.

Para que los mecanismos de demostración tengan un efecto real en la modificación de conductas de responsables y encargados, debe establecerse sistemas de supervisión por parte de la autoridad de control competente. Asimismo, deberán existir otros organismos que tengan el nivel adecuado de pericia en relación con el objeto del tratamiento y su especialización que, debidamente acreditados por el citado organismo de control, puedan también realizar supervisiones y apoyar al organismo de control, así como atender las diversas necesidades del sector. Para el efecto, deberá establecerse mecanismos de acreditación por parte de una autoridad competente, procedimientos para su aprobación y revocatoria de un organismo acreditado con pericia que realicen certificaciones y supervisiones que acrediten el cumplimiento de las operaciones de tratamiento de los responsables y los encargados, sobre todo de lo relativo a la privacidad por diseño y por defecto.

Finalmente, las autoridades de control de supervisión y de certificación deberán promover la protección de datos desde el diseño y, por defecto, con la finalidad de construir una cultura de

[1819] Argentina, Costa Rica, Nicaragua, República Dominicana y Uruguay.

protección de datos y motivar en conjunto con responsables y encargados que los consumidores, organizaciones y/o personas naturales seleccionen y usen productos, servicios y aplicaciones que estén basados en el tratamiento de datos personales por diseño y por defecto.

Artículo 67.- Obligaciones del responsable del tratamiento de datos personales.- El responsable del tratamiento está obligado a:

Tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;

Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;

Aplicar e implementar procesos de verificación, evaluación y valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas;

Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;

Adherirse a códigos de protección, mecanismos de certificación o sellos de protección de datos personales aprobados por la Autoridad de Protección de Datos Personales;

Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;

Realizar evaluaciones de adecuación al nivel de seguridad previa al tratamiento de datos personales;

Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;

Notificar a la Autoridad de Protección de Datos Personales y al titular de violaciones a las seguridades implementadas para el tratamiento de datos personales conforme a lo establecido en el procedimiento previsto para el efecto;
Implementar la protección de datos personales desde el diseño y por defecto;

Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;
Elegir y designar el encargado del tratamiento de datos personales que ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme lo establecido en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional;

Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, de conformidad a lo dispuesto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales;

Designar al Delegado de Protección de Datos Personales;

Permitir y contribuir a la realización de auditorías o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales; y,

Los demás establecidos en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

Artículo 68.- Obligaciones del encargado del tratamiento de datos personales.- El encargado del tratamiento de datos personales está obligado a:

Tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;

Tratar datos personales de conformidad a lo previsto en el contrato que mantenga con el responsable del tratamiento de datos personales, inclusive en lo que respecta a la transferencia o comunicación internacional, salvo que esté obligado a hacerlo en función al principio de legitimidad; de ser este el caso, deberá informar al responsable del tratamiento de datos personales;

Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el personal a cargo del tratamiento de datos personales, o con quién tenga conocimiento de los datos personales;

Garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;

Implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales a efecto de evitar vulneraciones;

Asistir al responsable para que éste cumpla con su obligación de atender solicitudes que tengan por objeto el ejercicio de los derechos del titular frente al tratamiento de sus datos personales;

Asistir al responsable para garantizar el cumplimiento de las obligaciones previstas en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;

Transferir o comunicar los datos personales entregados al responsable del tratamiento y suprimirlos, una vez que haya culminado su encargo;

Facilitar el acceso al responsable del tratamiento de datos personales de toda la información referente al cumplimiento de las obligaciones establecidas en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;

Permitir y contribuir a la realización de auditorías o inspecciones, por parte del responsable del tratamiento de datos personales o de un auditor autorizado por éste o por la Autoridad de Protección de Datos Personales;

Cumplir el código de protección, mecanismos de certificación o sellos aprobados para demostrar la existencia de garantías suficientes para la protección de datos personales; y,

Las demás establecidas en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

2.6.5 Contenido de las facultades que les corresponden a los titulares para el ejercicio del objeto

2.6.5.1 Derecho de acceso

La Ley Orgánica de Transparencia y Acceso a la Información Pública del Ecuador acata este derecho en la fórmula de Promoción del Derecho de Acceso a la Información, contenida en el octavo artículo, que regula a la información pública, el *habeas data* y el amparo. Las aseveraciones postuladas en Ecuador con respecto al *habeas data* sugieren que su espíritu fortifica la democracia ya que es una invitación a la transparencia del tratamiento y, por ende, al cumplimiento de las finalidades. Respecto del derecho de acceso con relación directa con el *habeas data* lo toma también Brasil y Honduras.

Varios países incluidos en este estudio se han permitido adoptar en su normativa, ya sea de manera intrínseca o expresa, este derecho. Por ejemplo, El Salvador, Chile, Paraguay y Venezuela.

Por su parte, el RGPD en el considerando (63) ha determinado el alcance de este derecho con relación a los datos personales recogidos que le conciernan al titular —como también lo adoptan los Estándares de Protección de Datos— y la importancia de resolverlo sin dificultad a fin de garantizar la licitud del tratamiento. Criterio que no siempre es compartido, así es por ejemplo en Venezuela, que determina su alcance en relación con documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas.

Por otro lado, el artículo 15 del mencionado reglamento de la Unión Europea refleja la relación entre el derecho de acceso con el deber de información, como lo resuelve también las Recomendaciones de la Organización de Estados Americanos Sobre Protección de Datos Personales. Relación que se evidencia también con el principio de finalidad, ya que por medio de estos el titular determinará en qué medida ejercer su derecho de acceso.

Por otra parte, el RGPD ha permitido establecer una serie de mecanismos —como también lo orienta El Salvador— mediante los cuales el titular goza de la disposición de una copia de datos personales por parte del responsable del tratamiento. Este último también tendrá derecho a solicitar ciertas condiciones para que el titular pueda acceder a este derecho. Por tanto, se puede brevemente concluir que para el RGPD la actuación del responsable es imprescindible en dos condiciones: el establecimiento de mecanismos y el derecho de exigir condiciones mínimas; esta última cualidad dota de una salvaguarda al responsable y limita cualquier posible actuar arbitrario por parte del titular del dato.

En el mismo contexto de las limitaciones, para la Unión Europea este derecho ha concebido una barrera esencial que lleva por nombre *interés general* —en una de sus acepciones—. En este contexto, el derecho de acceso podrá efectivizarse en la medida en que no afecte los derechos ni las libertades de terceros con especial énfasis en derechos de propiedad intelectual. Ahora bien, esta limitación en particular deberá ser estudiada de manera detenida para determinar si la negativa debe darse en relativo o en su totalidad.

En Latinoamérica se concentra la visibilidad de dos criterios en relación con este derecho, es así su espíritu preventivo como lo desarrolla Bolivia al definirlo como la acción de protección de la privacidad; por otra parte, Paraguay, Honduras y Bolivia destacan un espíritu reactivo que señala que se requiere de transgresiones a derechos como la intimidad, privacidad, entre otros, para poder alcanzar la efectivización de este derecho.

Al desarrollar Latinoamérica, también se reconoce que Argentina, Colombia, Costa Rica, Ecuador, Guatemala, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay establecen uniformemente el derecho de acceso a la información o datos personales, prestándose a cumplir con especiales características como la legitimidad, banco de datos, tratamiento, gratuidad —en concordancia con las Recomendaciones de la Organización de Estados Americanos Sobre Protección de Datos Personales— y finalmente, el procedimiento.

Una característica especial, adoptada por los Estándares de Protección de Datos, es que el acceso no se presta únicamente para los datos, sino incluso para los detalles del tratamiento.

Finalmente, las recomendaciones de la Organización de Estados Americanos sobre Protección de Datos Personales señalan que se encuentran incluidos tres derechos que se

manejan en la doctrina y en varias legislaciones latinoamericanas: derecho de acceso, derecho de rectificación y derecho de cesión.

> **Artículo 22.- Derecho de Acceso.-** El titular tiene derecho a conocer y a obtener del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna.
>
> El responsable del tratamiento de datos personales deberá establecer métodos razonables que permitan el ejercicio de este derecho.
>
> En caso de que fuera necesario restringir o negar dicho acceso, deberán especificarse las razones concretas de dicha restricción o negativa de acuerdo a lo establecido en la normativa vigente.

2.6.5.2 Derecho de rectificación

El derecho de rectificación en nuestro país tiene su origen en el *habeas data* y se conjuga, además, con la inicial introducción del derecho al acceso. Procede ante la existencia de data incorrecta, inexacta —como también lo ejecuta Chile, Honduras, El Salvador e incluso el GDPR—, aunque los datos también pueden ser obsoletos, tal y como fue observado a partir de sentencia ecuatoriana 46-2002.[1820]

Es importante mencionar que Ecuador importa un rasgo esencial respecto de este derecho: se lo confunde con el derecho a la libertad de expresión y, en consecuencia, con la esfera de los medios de comunicación. Ya que determina que se aplicará el derecho de rectificación, conforme señala la Constitución, como extensión del *habeas data* ya mencionado. No obstante, un rasgo significativo del derecho de rectificación que lo distingue del de rectificación, es la inclusión de medidas de reparación orientadas exclusivamente a subsanar el abusivo ejercicio del derecho a la libertad de expresión, por lo que, en Ecuador se debe hacer hincapié en identificar que el derecho de rectificación propio de la protección de datos personales es propio y distinto del de rectificación de una noticia o información noticiosa.

Por otra parte, el RGPD en el artículo 16 señala el derecho de rectificación, por el cual, se otorga al interesado el derecho a la modificar los datos personales, que pudieran ser inexactos, siempre y cuando los citados datos le conciernan, determinando como legitimado pasivo único al titular e invocando el principio de finalidad y el deber de información constatado en el posterior artículo 19.

Respecto de Latinoamérica, como fue revisado en el capítulo IV, todos los países objeto de estudio conciben este derecho con diferentes condiciones de aplicabilidad; en otras palabras, e procede únicamente cuando los datos son erróneos (Venezuela y Paraguay), además inexactos o incompletos (El Salvador y Chile) e inequívocos (Chile).

[1820] Ecuador, Tribunal Constitucional del Ecuador, *Sentencia 0046-2002-HD*, ROS, No. 66, 22 de abril de 2003; Ecuador, Corte Constitucional del Ecuador, *Sentencia 0051-08-HD*], ROS 137, 26 de noviembre de 2008; *Sentencia 0038-2008-HD*, ROS 133, 10 de julio de 2009.

Otras condiciones serían la ilegalidad y arbitrariedad acerca de lo que Bolivia respecta. Por otra parte, para Venezuela, Paraguay, Bolivia y Honduras se requiere un daño a derechos fundamentales. De modo que, con miras a ser concluyentes en el espacio latinoamericano, se deben cumplir una serie de condiciones, tales como: error o falsedad, incompletos o inexactos, que afecten derechos, que su tratamiento se encuentre expresamente prohibido o no autorizado.

Cabe agregar, para que opere la rectificación se deberá verificar que los datos personales sean necesarios o pertinentes, no esté vencido el plazo para su tratamiento; además, que se visibilice la constancia de esta revisión para que opere la limitación de tratamiento.

Respecto a la ejecución se han determinado parámetros que versen sobre lo gratuito y la negativa motivada a rectificación, además de aludir a una serie de excepciones como: que se pudieran obstaculizar actuaciones judiciales o administrativas en curso, el cumplimiento de obligaciones tributarias, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de crímenes y delitos por la autoridad competente, y la verificación de infracciones administrativas.

En ese sentido, los Estándares de Protección se han pronunciado respecto del derecho de rectificación, teniendo como base de nuevo al titular como legitimado activo y actuando frente a los datos que resulten ser inexactos, incompletos o no se encuentren actualizados.

Luego del análisis realizado, se pone en consideración el siguiente texto normativo:

> **Artículo 23.- Derecho de Rectificación y Actualización.-** El titular tiene el derecho de solicitar se corrijan o actualicen sus datos inexactos, incompletos, desactualizados, erróneos, falsos, incorrectos o imprecisos.

2. 6.5.3 Derecho de oposición

El RGPD asume el derecho de oposición en el artículo 21, exponiendo que el interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento, incluida la elaboración de perfiles.

Además, la citada norma menciona las condiciones de interposición de este derecho: cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines, a más tardar en el momento de la primera comunicación con el interesado; si se refieren a la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia. Asimismo, en el contexto de la utilización de servicios de la sociedad de la información en el sector de las comunicaciones electrónicas, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

De otro lado, también se impone una serie de condiciones que determinarán la posibilidad de que el responsable del tratamiento pueda retener los datos y mantener el tratamiento pese a la oposición del titular. Así, por ejemplo: a) cuando se acrediten motivos legítimos imperiosos que prevalezcan sobre los intereses, los derechos y las libertades del interesado; b) cuando estén asociados al cumplimiento de una misión realizada en interés público o en el ejercicio

de poderes públicos conferidos al responsable del tratamiento; c) cuando los datos personales puedan ser tratados lícitamente y son necesarios para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero; d) cuando el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, para la formulación y el ejercicio o la defensa de reclamaciones; e) cuando se traten con fines de investigación científica o histórica o con fines estadísticos.

Del análisis latinoamericano plasmado en el capítulo IV, se colegió que aquellos países que basan el sistema de protección de los datos personales desde el derecho a la intimidad o a la privacidad no reconocen el derecho de oposición, que es contenido propio del derecho a la autodeterminación informativa. En este sentido, El Salvador, Bolivia, Honduras, Paraguay y Venezuela no incluyen este derecho. En cambio, países como Chile y Brasil reconocen que el consentimiento puede ser revocado; esta es una forma indirecta de aplicación de este derecho; sin embargo, no está reconocido como tal. Hay normativas además que lo han asociado con el deber de información y con la revocatoria del consentimiento.

Hemos revisado en ese sentido que los dos parámetros que cubren la orientación de este derecho se basan, con respecto a la ejecución antes tratada por el RGPD, en estamentos como la negativa a la oposición y el cese del tratamiento o supresión.

Los Estándares de Protección también han determinado que mediante este derecho, el titular podrá oponerse al tratamiento de sus datos personales cuando tenga una razón legítima derivada de su situación particular o el tratamiento de sus datos personales; cuando tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad.

De lo analizado, la propuesta de norma es la siguiente:

> **Artículo 25.- Derecho de oposición.-** El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en especial para fines de mercadotecnia, valoraciones o decisiones automatizas incluida la elaboración de perfiles.

2. 6.5.4 Derecho de cancelación y anulación

No existe uniformidad sobre la denominación de este derecho, el RGPD lo denomina supresión, como algunos países latinoamericanos,[1821] otros lo llaman cancelación[1822] y otros, eliminación.[1823] Únicamente Guatemala no lo reconoce en su normativa. Adicionalmente, varios países, entre ellos Ecuador, incluyen un derecho que puede ser considerado diferente por sus consecuencias, titulado anulación. Otras normativas incluyen dentro del derecho de cancelación también al derecho de bloqueo.

[1821] Argentina, Colombia, Costa Rica y Nicaragua.
[1822] México y Uruguay.
[1823] Panamá, Perú, Ecuador y República Dominicana.

En todo caso, el criterio generalmente aceptado, independientemente del nombre que se le haya asignado, es considerarlo un derecho del titular[1824] que faculta la supresión de los datos personales, sin dilación indebida de los archivos, registros, expedientes y sistemas del responsable,[1825] cuando se cumplen ciertas circunstancias que se analizan a continuación, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados.[1826]

Los citados criterios que justifican una eliminación o supresión de datos personales son:

b) Que afecten derechos: En este sentido constan las legislaciones de Colombia, Ecuador y Nicaragua que determinan expresamente que pueden eliminarse datos personales cuando afecten los derechos del titular.

c) *Revocatoria del consentimiento:* Cuando el interesado ha retirado el consentimiento para uno o varios fines específicos (art. 6, num. 1, lit. a), RGPD), o cuando el interesado dio su consentimiento explícito para el tratamiento de datos sensibles con uno o más de los fines especificados, y este no se base en otro fundamento jurídico que permita retenerlos al responsable del tratamiento (art. 9, num. 2, lit. a), RGPD).

d) *Cuando ha expirado la vigencia del tratamiento:* Perú señala que pueden ser eliminados datos personales cuando se hubiera vencido el plazo establecido para su tratamiento.

e) *Cuando se ha cumplido con la finalidad del tratamiento:* Esto es cuando los datos personales ya no son necesarios para la finalidad para los que fueron recogidos. Perú y Costa Rica consideran como condición para eliminar datos personales que hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recopilados.

f) *Cuando se ha incumplido el principio tratamiento legal y transparente y de lealtad:* Esto es que se ha tratado datos de manera distinta a la que se solicitó su autorización inicial y no se haya recibido consentimiento del titular respecto de esta nueva finalidad (art. 17, RGPD), o cuando los datos personales hayan sido tratados ilícitamente, es decir se haya faltado al principio de legalidad y tratamiento legal y transparente.

g) *Cuando el dato sea inexacto:* El dato podrá ser rectificado o eliminado si el dato es inexacto por incompleto o desactualizado. En el caso de Perú y República Dominicana únicamente es invocable este derecho en este caso particular: cuando los datos sean inexactos o incompletos.

h) *Cuando el dato sea errado o falso:* El dato podrá ser rectificado o eliminado si el dato es errado o falso. Argentina, Ecuador y Perú señalan que es invocable este derecho en este caso particular: cuando los datos sean errados o falsos.

i) *Cuando no exista autorización legítima:* Cuando se requiera la autorización de la ley o el titular y no se cuente con ella.

j) *Datos de niños, niñas y adolescentes:* Cuando se hayan obtenido datos personales en relación con la oferta de servicios de la sociedad de la información de niños menores de 16, sin la autorización de quien ostenta la patria potestad o tutela; o de menos de 13 años, si en el país existe una norma que establezca esta edad como la mínima necesaria para la capacidad jurídica.

[1824] República Dominicana y Costa Rica establecen que, además de un derecho del titular, es una obligación del responsable del tratamiento.
[1825] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1826] Ibíd.

k) *Cuando el titular se oponga al tratamiento:* Se podrá eliminar datos personales cuando el interesado se opone al tratamiento de datos personales que les conciernen (considerando [65], RGPD), siempre y cuando no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2.

En ese sentido, en concordancia con el RGPD, existen excepciones al derecho de cancelación que posibilitan la retención lícita de los datos personales por parte del responsable del tratamiento cuando:

a. para ejercer el derecho a la libertad de expresión e información;

b. para el cumplimiento de una obligación legal o deber legal o contractual que lo impida, como el caso de Colombia;

c. para el cumplimiento de una misión realizada en interés público, por ejemplo en el ámbito de la salud pública, es decir para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social; gestión de los sistemas y servicios de asistencia sanitaria y social, la protección frente a amenazas transfronterizas graves para la salud; para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios; o cuando sea realizado por un profesional sujeto a la obligación de secreto profesional (art. 9, num. 2, lits. h) e i), y num. 3, RGPD). Por su parte, Argentina, México, Nicaragua y Uruguay establecen excepciones por las cuales el derecho de cancelación no puede cumplirse, en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando;

d. en el ejercicio de poderes públicos conferidos al responsable; por razones de interés público en el ámbito de la salud pública;

e. con fines de archivo en interés público, fines de investigación científica o histórica o con fines estadísticos (art. 89, apdo. 1, RGPD), en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento;

f. por disposición de la ley deban mantenerse en registros públicos, como en el caso de Ecuador;

g. para la formulación, el ejercicio o la defensa de reclamaciones;

h. existen posibles responsabilidades del tratamiento durante el plazo de prescripción de las obligaciones, pero cumplido el plazo, deberá procederse a la supresión, como ocurre con la normativa de República Dominicana;

i. la eliminación pudiese causar perjuicios a derechos o intereses legítimos de terceros, como ocurre con la normativa de República Dominicana;

j. existiera una obligación legal de conservar los datos, como ocurre con la normativa de República Dominicana;

k. se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de crímenes y delitos por la autoridad competente y la verificación de infracciones administrativas, al tenor de la normativa de Argentina;

l. exista una resolución judicial que lo determine, conforme señala la normativa de Nicaragua y Argentina;

m. si el solicitante no es titular de los datos personales, o el representante legal no esté debidamente acreditado, no se encuentren los datos personales del solicitante en la base de datos, condiciones de formalidad contempladas en la normativa Argentina;

n. se obstaculice las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias, señalado en la normativa uruguaya.

Si bien, el RGPD consagra en el mismo artículo el derecho al olvido, en este estudio por haberlo estudiado en forma autónoma se lo analizará en el respectivo acápite.

Respecto de la operatividad de la eliminación debe resaltarse lo dispuesto en la normativa latinoamericana que señala que:

a) no tendrá costo para el titular la eliminación del dato personal, al tenor de lo dispuesto en Argentina, Colombia, Costa Rica, Ecuador, México, Nicaragua y Uruguay;

b) que antes de tomar la decisión de eliminar un dato y durante el tiempo de deliberación de esta decisión, el dato personal debe bloquearse y dejar constancia de ello para informar por qué no puede ser usado, conforme la normativa Argentina, Colombia, Costa Rica, México, Nicaragua y Uruguay establecen;

c) que la comunicación de datos a un tercero debe ser detenida cuando los datos se eliminan de la base original, y además debe reportarse al tercero para que también los elimine de la suya, esto es el caso de Argentina y Uruguay.

En Ecuador, el derecho de eliminación no consta de manera expresa en el numeral 19 del artículo 66 de la CRE, ya que si bien se puede identificar al derecho de acceso, no existe mención alguna sobre los otros derechos como el de rectificación, cancelación y oposición. La norma en mención únicamente señala que el derecho a la protección de datos personales incluye el acceso, la decisión sobre información y datos de este carácter, así como su correspondiente protección, por lo que en esta última frase se puede colegir que otro mecanismo de protección es la supresión o eliminación.

Mención expresa a este derecho si consta en la acción de *habeas data*, artículo 92 de la CRE y artículo 49 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, cuya finalidad es el acceso a los datos para ejercitar el derecho a la autodeterminación informativa

o para la implementación de los derechos de rectificación, cancelación y anulación, con miras a evitar actos discriminatorios o perjuicios relacionados con la transgresión de otros derechos fundamentales como el honor, la intimidad y, ahora, la protección de datos personales.

Específicamente el derecho de cancelación procede cuando "los datos son innecesarios para la finalidad del fichero o sean excesivos en relación con la misma",[1827] cuando los datos fueren erróneos o afecten sus derechos; o cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente,[1828] por lo tanto, es menester anular, borrar, hacer ilegible, destruir o dejar irreconocibles los datos.

Condiciones de aplicación general del derecho de acceso, por medio de la garantía constitucional del *habeas data*, son las siguientes:

a) No podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos.

b) La persona titular de los datos podrá solicitar al responsable, sin costo el acceso, la actualización, rectificación, eliminación o anulación (art. 92, CRE; art. 49, LOGJCC).

Una aplicación específica, en un ámbito limitado a registros públicos, se encuentra prevista en el artículo 21 de la Ley del Sistema Nacional de Registro de Datos Públicos,[1829] que en la parte pertinente dispone: "La o el titular de los datos podrá exigir las modificaciones en registros o bases de datos cuando dichas modificaciones no violen una disposición legal, una orden judicial o administrativa. La rectificación o supresión no procederá cuando pudiese causar perjuicios a derechos de terceras o terceros, en cuyo caso será necesaria la correspondiente resolución administrativa o sentencia judicial". De esta manera, por modificaciones se entienden también aquellos datos que deben ser eliminados, anotándose que deben cumplirse criterios de protección frente a terceros o de cumplimiento de disposiciones legales, judiciales para su procedencia.

Finalmente, el citado artículo 92 de la Constitución señala el derecho de anulación, cuyo efecto es volver todo al estado anterior como si el daño no se hubiese producido. Por eso, en la consecuencia es que radica su diferencia con el derecho de supresión. Como consta en la normativa constitucional ecuatoriana, se vuelve necesario incluirla en el texto de una ley de protección de datos con la finalidad de guardar una adecuada armonía en la normativa ecuatoriana vigente.

> **Artículo 24.- Derecho de eliminación.-** El titular tiene derecho a solicitar la supresión de sus datos personales, a fin de que estos dejen de ser tratados por el responsable del tratamiento de datos personales, cuando:
>
> a) El tratamiento no cumpla con los principios de juridicidad, lealtad, transparencia y legitimidad;

[1827] A. HERRÁN ORTÍZ, *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales* (Madrid: Dykinson, 2002), 288.
[1828] Artículo 50, *Ley Orgánica de Jurisdicción y Control Constitucional del Ecuador*.
[1829] Asamblea Nacional Ecuador, *Ley 0, Ley del Sistema Nacional de Registro de Datos Públicos*, Registro Oficial Suplemento 162, 31 de marzo de 2010, Ultima modificación: 12 de septiembre de 2014.

b) El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad;

c) Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;

d) Haya vencido el plazo de conservación de los datos personales;

e) El tratamiento afecte derechos fundamentales o libertades individuales; o

f) Haya revocado o no haya otorgado el consentimiento para uno o varios fines específicos, sin necesidad de que medie justificación alguna.

El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a eliminar, anular, borrar, hacer ilegible, destruir o dejar irreconocibles de forma definitiva y segura.

Artículo 26.- Derecho de anulación.- El titular tiene derecho a solicitar la nulidad ante autoridad jurisdiccional por ilicitud en el acto o el tratamiento de datos personales, bajo las causales señaladas para la nulidad en materia civil, mercantil y administrativa, según sea el caso.

2. 6.5.5 Derecho a no soportar valoraciones producto de procesos automatizados que afecten derechos fundamentales

El RGPD determina que el interesado tiene derecho a no ser objeto de una decisión basada únicamente en un tratamiento automatizado destinado a valorar o evaluar, sin intervención humana,[1830] determinados aspectos personales del mismo, o analizar o predecir, incluida la elaboración de perfiles, aquella información relacionada con su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad, conductas o comportamientos, rendimiento laboral, crédito; que produzcan efectos jurídicos en él o afecte derechos,[1831] o le afecte significativamente sus intereses, derechos o libertades.[1832] Por ejemplo, "la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna" (considerando [71], RGPD).

Conforme señalan el RGPD y los Estándares Iberoamericanos de Protección de Datos Personales, este derecho incluye varias garantías y medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado como las de: a) obtener la intervención humana; b) recibir una explicación sobre la decisión tomada; c) expresar su punto de vista; d) impugnar la decisión[1833] constante en actos administrativos o decisiones

[1830] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.

[1831] México, por su parte, establece efectos jurídicos no deseados o que afecte de manera significativa sus intereses, derechos o libertades.

[1832] Uruguay y Perú señalan que el proceso de automatización afecta significativamente al titular.

[1833] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*. Uruguay también lo reconoce en la *Ley 18.331, de Protección de Datos Personales y Acción de Habeas Data*, 11 de agosto de 2008, D.O. 18 de agosto de 2008 - 27549.

privadas que impliquen una valoración automatizada de su comportamiento,[1834] e) derecho a conocer información del responsable de la base de datos, tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento automatizado, este derecho está reconocido en la normativa uruguaya,[1835] f) garantizar un tratamiento leal y transparente, g) tener en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, h) utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, i) aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, aquellas que corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, i) asegurar los datos personales de los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto.[1836]

Este derecho ha sido reconocido de manera heterogénea en Argentina, Perú, México y Uruguay. Únicamente Argentina determina que las decisiones automatizadas deben ser judiciales o relativas a actos administrativos; en las otras legislaciones citadas el ámbito de cobertura no es limitado, sino que puede aplicar a cualquier tipo de decisión.

El Estándar Iberoamericano de Derecho a la Protección de Datos Personales señala que este derecho no procede cuando: a) sea necesario para la negociación,[1837] celebración o la ejecución de un contrato entre el titular y el responsable, por ejemplo para para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento;[1838] b) esté autorizado por la ley, siempre que se establezca medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, por ejemplo para fines de control y prevención del fraude y la evasión fiscal; c) se base en el consentimiento demostrable o explícito[1839] del titular; por su parte la legislación peruana añade también a la evaluación con fines de incorporación a una entidad pública, sin perjuicio de la posibilidad de defender su punto de vista, para salvaguardar su legítimo interés.[1840]

El responsable no podrá llevar a cabo tratamientos automatizados de datos personales de menores de edad,[1841] tampoco de aquellos que tengan como efecto la discriminación de los titulares por su origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, así como datos genéticos o datos biométricos.[1842]

Pero podrá tratar datos sensibles, cuando haya tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado y se cumplan una de las

[1834] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, *Ley 18.331, de Protección de Datos Personales y Acción de Habeas Data*, 11 de agosto de 2008, D.O. 18 de agosto de 2008 - Nº 27549.
[1835] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General.
[1836] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.
[1837] Congreso de la República del Perú, *Ley 29733, de Protección de Datos Personales*, 3 de julio de 2011.
[1838] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016..
[1839] Ibíd.
[1840] Congreso de la República del Perú, *Ley 29733, de Protección de Datos Personales*, 3 de julio de 2011.
[1841] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.
[1842] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.

siguientes condiciones: a) se aplique consentimiento explícito; b) el tratamiento es necesario por razones de un interés público esencial, que debe ser proporcional al objetivo perseguido; c) establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.[1843]

Respecto de los efectos jurídicos de los actos basados en estas decisiones automatizadas que no han cumplido con los criterios de garantía y protección, serán insanablemente nulos, como forma de salvaguardar los derechos del titular.

Finalmente, Uruguay establece, como protección positiva, que la valoración sobre el comportamiento de las personas podrá tener valor probatorio únicamente a petición del afectado.

> **Artículo 37.- Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas en categorías especiales de datos.-** Además de los presupuestos establecidos en el artículo 30 de la presente Ley, no se podrán tratar datos sensibles o datos de niñas, niños y adolescentes, a menos que se cuente con autorización explícita del titular o representante legal; o, cuando dicho tratamiento esté destinado a salvaguardar el interés público.

2. 6.5.6 Derecho de consulta al registro general de protección de datos personales

Este derecho es especial y únicamente tratado en el RGPD en el artículo 30 que declara que el responsable, encargado o sus representantes, de ser el caso, tienen la obligación de realizar un registro de bases de datos efectuado bajo su responsabilidad, para ponerlo a disposición de la autoridad de control que en su momento lo solicite.

De otro lado, los titulares de datos personales tienen derecho a consultar registros realizados ante las autoridades de control de cada país. Así está reconocido en Argentina, Colombia, Costa Rica, Guatemala, Perú, Nicaragua y Uruguay (véase numeral 2.5.5.11 del capítulo IV de este estudio). Por su parte, el RGPD establece que el registro ya no se realiza ante la autoridad de control, sino por el propio responsable. Cabe indicar que el numeral 5 del artículo 30 del RGPD señala que cuando la finalidad del registro es la consulta por parte de personas, solo podrán hacerlo los que tengan un interés legítimo.

Es parte también de esta norma la determinación de las características necesarias para la realización del Registro, esto es la necesidad de constancias relativas al nombre y datos de contacto del responsable del corresponsable, del representante y del delegado de protección de datos; los fines del tratamiento; las categorías de interesados, la naturaleza de los datos personales; la determinación de los destinatarios a quienes se comunicará los datos personales, incluidas la identificación de un tercer país si los datos son transfronterizos, los plazos previstos para la supresión de las diferentes categorías de datos, las medidas técnicas y organizativas de seguridad, apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

[1843] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.

Finalmente, como previamente se mencionó, el RGPD ha considerado la aplicación de mecanismos eficaces, esto en sustitución a las obligaciones generales de notificación indiscriminada que, en facto, no resultaban adecuadas.

A continuación consta el texto de la normativa propuesta para desarrollar este tema:

> **Artículo 85.- Registro Nacional de Protección de Datos Personales.-**El responsable del tratamiento de datos personales deberá reportar a la Autoridad de Protección de Datos, lo siguiente:
>
> a) Identificación de la base de datos o del tratamiento;
>
> b) El nombre, domicilio legal y datos de contactabilidad del responsable y encargado del tratamiento de datos personales;
>
> c) Características y finalidad del tratamiento de datos personales;
>
> d) Naturaleza de los datos personales tratados;
>
> e) Identificación, nombre, domicilio legal y datos de contactabilidad de los destinatarios;
>
> f) Modo de interrelacionar la información registrada;
>
> g) Medios utilizados para implementar los principios, derechos y obligaciones contenidas en la presente ley y normativa especializada;
>
> h) Requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas para garantizar la seguridad y protección de datos personales;
>
> i) Tiempo de conservación de los datos;
>
> j) Transferencias internacionales;
>
> k) Constancia de la existencia de códigos de conducta; y,
>
> l) Constancia de disponibilidad de certificaciones, sellos y marcas de protección de datos personales;
>
> Este registro deberá mantenerse actualizado en todo momento, de esta manera se controlará que ningún responsable o encargado del tratamiento de datos personales trate datos personales con fines y características distintas a las declarados en el registro o contratarías a la ley y normativa especializada en la materia.

2. 6.5.7 Derecho a indemnización por daños causados

El RGPD establece como derecho una consecuencia de la atribución de responsabilidad por el incumplimiento de una obligación. Desde esta perspectiva se prevé que toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de un tratamiento, en infracción de la ley, incluidas las violaciones de normas corporativas relativas al procesamiento de datos basados en un tratamiento automatizado, o en la elaboración de

perfiles, tiene derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

Por su parte, los Estándares Iberoamericanos de Protección de Datos Personales sugieren que la normativa interna determine la autoridad competente para conocer de este tipo de acciones, así como los plazos, requerimientos y términos por medio de los cuales será indemnizado este, en caso de resultar procedente.[1844]

Consecuente con ese criterio, el RGPD establece que este derecho podrá ser reclamado por vía judicial mediante una tutela judicial efectiva, sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control.

Para una correcta retribución de la responsabilidad, y por lo tanto de las indemnizaciones que esto impone, se ha previsto que el responsable o encargado, que participen en el mismo tratamiento, deberán considerarse como responsables de la totalidad de los daños y perjuicios, a efectos de que el titular pueda reclamar a cualquiera de ellos, puesto que es necesario garantizar una indemnización total y efectiva del interesado que sufrió los daños y perjuicios.

Sin perjuicio que, puede prorratearse en función de la responsabilidad de cada responsable o encargado por los daños y perjuicios causados por el tratamiento, todo responsable o encargado que haya abonado la totalidad de la indemnización puede interponer recurso posteriormente contra otros responsables o encargados que hayan participado en el mismo tratamiento.

Ahora bien, el responsable o el encargado deben quedar exentos de responsabilidad si se demuestra que no son responsables de modo alguno de los daños y perjuicios.

En el mismo sentido, Colombia, Costa Rica y Panamá consideran que ante el incumplimiento de la normativa por parte del responsable, el titular tiene derecho a demandar por vía civil la indemnización por los daños y perjuicios causados.

Mientras que Argentina, Ecuador, Guatemala, México, Nicaragua, Perú, República Dominicana y Uruguay determinan que, además de las responsabilidades civiles, proceden responsabilidades administrativas y penales.

De otro lado, Nicaragua, México y Guatemala reconocen expresamente que los procedimientos administrativos correspondientes son independientes de los del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

De lo visto, es por vía civil que después de una atribución debida de responsabilidad producto de una transgresión de una obligación constante en una norma que ha causado daño a la persona, el titular puede reclamar la correspondiente indemnización por daños y perjuicios.

Panamá es el único país que señala que no solo existen daños causados por responsables por su incumplimiento con la normativa de protección, sino también de los funcionarios por negar el acceso a los datos personales,

[1844] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.

En el caso del Ecuador, la norma, por su redacción amplía y general determina que los daños pueden ser causados, tanto por el responsable del tratamiento como por el funcionario público en el ejercicio de sus funciones.

Ecuador recoge la acción de *habeas data* como garantía constitucional con la cual se puede reclamar por el incumplimiento de las obligaciones propias del responsable o encargado del tratamiento de datos personales, o incluso al funcionario que no haya cumplido con sus responsabilidades.

La acción de *habeas data*, recogida en el artículo 92 de la Constitución de la República del Ecuador, señala que la persona afectada podrá demandar por los perjuicios ocasionados por un inadecuado tratamiento de sus datos personales. Ahora bien, este artículo debe ser leído e integrado con el 86 de la Constitución de República del Ecuador, que determina que el juez de la causa deberá ordenar la reparación integral, material e inmaterial y especificar e individualizar las obligaciones, positivas y negativas, a cargo del destinatario de la decisión judicial, y las circunstancias en que deban cumplirse.

Por su parte, el artículo 49 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (LOGJCC) señala que el concepto de reparación integral incluirá todas las obligaciones materiales e inmateriales que el juez determine para hacer efectiva dicha reparación. Norma que coincide con el artículo 18 de la misma ley que determina que en virtud de la reparación integral "podrá incluir, entre otras formas, la restitución del derecho, la compensación económica o patrimonial, la rehabilitación, la satisfacción, las garantías de que el hecho no se repita, la obligación de remitir a la autoridad competente para investigar y sancionar, las medidas de reconocimiento, las disculpas públicas, la prestación de servicios públicos, la atención de salud".

En consecuencia, Ecuador es el único país que hace referencia a la reparación integral, como consecuencia directa de una sentencia positiva dentro de un proceso relativo a la garantía constitucional de *habeas data*, por la que se reconoce no solo la indemnización por daños y perjuicios materiales como: el daño emergente, lucro cesante, proyecto de vida, costas y gastos; así como daños inmateriales,[1845] y además otras formas de reparación propias del sistema de defensa de derechos humanos como son las medidas de satisfacción[1846] (que buscan reparar el daño inmaterial, que no tienen alcance pecuniario) y las garantías de no repetición[1847] (medidas de alcance o repercusión pública), conforme ha señalado en varias resoluciones la Corte Interamericana de Derechos Humanos: Blanco Romero y otros; García

[1845] "El daño inmaterial puede comprender tanto los sufrimientos y las aflicciones causados a las víctimas directas y a sus allegados, como el menoscabo de valores muy significativos para las personas, así como las alteraciones, de carácter no pecuniario, en las condiciones de existencia de la víctima o su familia". Corte Interamericana de Derechos Humanos, "Caso Gómez Palomino vs. Perú", 22 de noviembre de 2005, supra nota 11, párr. 130.

[1846] Obligación de investigar los hechos denunciados, identificar, juzgar y sancionar a los responsables. Obligación de buscar los restos mortales de la víctima y entregarlos a sus familiares. Publicación de Sentencia de la Corte. Asistencia médica y psicológica. Corte Interamericana de Derechos Humanos, "Caso Gómez Palomino vs. Perú». *Reconocimiento simbólico [por parte del Estado] destinado a la recuperación de la memoria histórica de las personas desaparecidas.* Corte Interamericana de Derechos Humanos, "Caso Blanco Romero y Otros vs. Venezuela", 28 de noviembre de 2005. Ser objeto de una satisfacción de carácter moral públicamente y con trascendencia. (Disculpas públicas) Corte Interamericana de Derechos Humanos, "Caso García Asto y Ramírez Rojas", 25 de noviembre de 2005.

[1847] *Programa de educación. Reformas normativas* locales. Corte Interamericana de Derechos Humanos, "Caso Gómez Palomino vs. Perú".

Asto y Ramírez Rojas; y Gómez Palomino, es decir que intenten volver a la situación anterior al daño en la medida de lo posible mediante una reparación integral.

Resta analizar si esta forma integral de afrontar la responsabilidad es extensible a los resultados de reclamaciones administrativas, civiles y penales, ante lo cual por el principio de aplicación directa de la Constitución ecuatoriana constante en el artículo 11, numeral 3, se concluye que rige cualquiera de los procesos descritos, de modo que las autoridades y jueces deben incluirlos en el texto de sus correspondientes resoluciones. Por lo que el derecho de indemnización debe entenderse aplicable en un estándar alto de protección. La normativa propuesta es la siguiente:

2. 6.5.8 Derecho a confidencialidad

Dentro del contexto ecuatoriano, el derecho de confidencialidad se indica de manera intrínseca, frente al análisis previamente realizado, respecto a datos sensibles. Así, el artículo 6 de la Ley del Sistema Nacional de Registro de Datos Públicos eleva un sistema de protección especial, en este caso la condición de confidencialidad, al disponer que sean confidenciales o reservados aquellos datos atinentes a la intimidad personal.

En consecuencia, el acceso a estos datos solo será posible con autorización expresa del titular de la información como lo disponen normativas como la de Perú, Colombia, Nicaragua y Uruguay; por mandato de la ley, como señala Argentina, Colombia y Uruguay; o por orden judicial, como dispone Argentina, Costa Rica, Nicaragua, Perú, República Dominicana y Uruguay. Añadiéndose que existe divergencia entre considerar a la confidencialidad como principio o como derecho, a criterio de este estudio cuenta con ambas condiciones, pues es una prerrogativa del titular y una obligación general de aplicación por parte del responsable del tratamiento.

En ese contexto se ha determinado como primera excepción el consentimiento del titular, aunque también debe estar justificado y siempre por el interés general. Además, se añade la obligatoriedad, por parte de quien trata la información, de implementar mecanismos que favorezcan su confidencialidad. En materia de excepciones para tratar datos personales, se logró concluir que en Latinoamérica no podrán reservarse los datos relativos a: a) fuentes de información periodística para Argentina; b) datos que tengan la naturaleza de públicos para Colombia; c) de interés social para Nicaragua; d) para la defensa nacional, seguridad pública o la sanidad pública en Perú y República Dominicana.

Se puede concretar con respecto a la implementación de mecanismos que el derecho de confidencialidad aparece directamente relacionado con el derecho de seguridad, ya que es obligación del responsable realizar una evaluación de riesgos que determine en qué condiciones se implementarán los mecanismos adecuados, criterio compartido por el RGPD en el considerando (39). Además, el ya mencionado reglamento determina los llamados niveles de confidencialidad en función a la sensibilidad de la data.

Latinoamérica, por su parte, como se analizó en el capítulo cuarto, comparte el criterio de confidencialidad de la data sensible, conforme es señalado por Honduras, Brasil y El Salvador, a lo cual se añade que entre los tipos de datos considerados sensibles constan los de

niños, niñas y adolescentes por los cuales en El Salvador se menciona la autorización de sus representantes.

Otro punto importante considerado por Bolivia, Argentina, Colombia, Costa Rica, México, Perú y Uruguay y Chile —aunque este último lo extiende al secreto— es la importancia de mantener este derecho aun después de haber concluido con el tratamiento y el vínculo con el titular. Además, vale la pena anotar la precisión que realiza la normativa de Costa Rica al señalar que el personal técnico y administrativo de la autoridad de control está obligado a guardar secreto profesional y deber de confidencialidad de los datos de carácter personal que conozca en el ejercicio de sus funciones.

Por su parte, la OEA establece en el Principio 5 que el deber de confidencialidad consiste en que "los datos personales no deben divulgarse, ponerse a disposición de terceros, ni emplearse para otros propósitos que no sean aquellos para los cuales se obtuvieron, excepto con el conocimiento o consentimiento de la persona en cuestión o bajo autoridad de la ley".[1848]

De lo analizado, se puede poner en consideración la siguiente propuesta normativa:

> **Artículo 14.- Confidencialidad.-** El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no deben tratarse o comunicarse para un fin distinto para el cual fueron recogidos, sin que se cuente con el consentimiento del titular o concurra una de las causales que habiliten el tratamiento conforme al principio de legitimidad. El nivel de confidencialidad dependerá de la naturaleza del dato personal.
>
> Este principio no implica solamente el mantenimiento de la seguridad de los datos personales, sino también la facultad del titular de controlar la forma en la que se tratan sus datos, incluyendo la transferencia o comunicación.

2. 6.5.9 Derecho al olvido digital

Los antecedentes más remotos del derecho al olvido se remontan a la resolución de la Corte Suprema Italiana de 1998, la cual estableció como "justo interés de toda persona a no quedar indefinidamente expuesta a los daños ulteriores que producen a su honor y a su reputación la publicación reiterada de una noticia que en el pasado fue legítimamente divulgada".[1849]

De otro lado, Francia en el año 2010 dirigió una consulta pública a sus ciudadanos y empresas mediante la cual les preguntó sobre si desean acogerse voluntariamente al olvido digital de la publicidad dirigida y en los sitios colaborativos y en los motores de búsqueda. Como era de esperarse, ni Google ni Facebook aceptaron esta propuesta.[1850]

[1848] Asamblea General OEA, 86 Período Ordinario de Sesiones, CJI/doc. 474/15 rev.2 Río de Janeiro, Brasil, 26 marzo 2015, *Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales*, http://www.oas.org/es/sla/ddi/docs/cji-doc_474-15_rev2.pdf.

[1849] Sentencia de 9 de abril de 1998, Corte Suprema italiana citada en Loreto Carmen Mate Satué, «¿QUÉ ES REALMENTE EL DERECHO AL OLVIDO?», accedido 31 de octubre de 2018, file:///C:/Users/Lorena/Downloads/163-938-1-PB%20(1).pdf.

[1850] Corte Suprema de Italia, citada en Loreto Carmen Mate Satué, "Sentencia de 9 de abril de 1998".

Pero sin duda, el hito en el reconocimiento del derecho al olvido se encuentra en la sentencia C-131/12 entre Mario Costeja González y la Agencia Española de Protección de datos en contra de Google INC y Google Spain SL[1851] ante el Tribunal de Justicia de la Unión Europea. En esta resolución se reconoce por primera vez este derecho al señalar que Google debía eliminar u ocultar los datos personales del reclamante para que dejaran de incluirse en sus resultados de búsqueda y no estuvieran ligados a los enlaces del periódico *La Vanguardia*, en los cuales se hacía referencia a dos anuncios sobre una subasta de inmuebles relacionada con un embargo derivado de deudas, porque a criterio del titular, esta información le perjudicaba toda vez que ya se encontraba rehabilitado de su condición de deudor.

De lo visto, el análisis de aplicación de este derecho depende directamente del principio de ponderación, por el cual se determina un equilibrio entre el derecho a la vida privada, la protección de datos personales del perjudicado y la libertad de expresión, de información o consideraciones como el interés público o la memoria histórica. En consecuencia, es necesario un análisis pormenorizado por parte de los jueces, quienes deben verificar si existe una adecuada ponderación de derechos.

De manera general, los criterios que deben ser parte del análisis de los jueces son: a) la relevancia de la información para una comunidad; b) la utilidad de la información en orden de conocer aspectos relevantes de su entorno o para contribuir en la generación de una opinión del internauta; c) un impacto en la vida privada limitado; d) si existe una obligación que le implique soportar limitaciones a sus derechos; e) si ha transcurrido tiempo suficiente; y, f) si exista un justo equilibro entre el interés legítimo de internauta y los derechos de los titulares de datos personales.

Ahora bien, México plantea una postura contraria al derecho al olvido, desde la visión constante en la resolución dictada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, por el cual en un proceso sancionatorio contra Google México un ciudadano, Carlos Sánchez Peña, solicitó derecho al olvido. La resolución fue recurrida por la Red de Defensa de los Derechos Digitales. En la resolución del recurso de revisión por parte del Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región no se permitió la aplicación del derecho al olvido por cuanto se consideró que en este caso primaba el derecho a la libertad de expresión contra el derecho al olvido, ya que la información que se intentaba eliminar de la indexación era la relativa a resultados de búsqueda que relacionaban su nombre con un fraude con dineros públicos.

De lo visto, es necesario que la aplicación del derecho al olvido digital se analice individualmente, en vía judicial, ya que solo un juez puede realizar una adecuada ponderación de derechos fundamentales.

El derecho al olvido se asociaba exclusivamente a la desindexación de información no relevante, sin repercusión en la memoria histórica ni afectación a la libertad de expresión que, sin embargo, causaba transgresiones a los derechos del titular. Ahora bien, el RGPD lo reconoce expresamente en el mismo artículo relativo al derecho de supresión, debido a que

[1851] Tribunal de Justicia de la Unión Europea, "Asunto C-131/12, en el caso Google Spain y Google", 2014, http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES.

son las mismas circunstancias las que habilitan o no el derecho de cancelación y el derecho al olvido.

Las citadas circunstancias por las cuales un responsable que haya hecho públicos datos personales está obligado a eliminar los datos personales son: la trasgresión a los principios de finalidad, licitud, lealtad, transparencia, consentimiento, entre otros. Cabe destacar que, de proceder la supresión, debe ampliarse para que el responsable del tratamiento que haya hecho públicos los datos personales esté obligado a indicar a los responsables del tratamiento que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Para lo cual, el responsable del tratamiento deberá tomar en cuenta la tecnología disponible y el coste de su aplicación y adoptar medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos (considerando [66] y en núm. 2, art. 17, RGPD).

El mismo RGPD establece que no procederá ni el *derecho de cancelación, ni el derecho al olvido* y posibilita la retención lícita de los datos personales por parte del responsable del tratamiento cuando es necesario para: a) permita el ejercicio del derecho a la libertad de expresión e información; b) permita el cumplimiento de una obligación legal de un responsable del tratamiento; c) el cumplimiento de una misión realizada en interés público; d) el ejercicio de poderes públicos conferidos al responsable; e) el interés público en el ámbito de la salud pública, es decir para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios; o cuando sea realizado por un profesional sujeto a la obligación de secreto profesional; f) fines de archivo en interés público, fines de investigación científica o histórica, o fines estadísticos si pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, g) para la formulación, el ejercicio o la defensa de reclamaciones.

En Latinoamérica, sobre derecho al olvido, se tienen distintas formas de concebirlo, puesto que hay países donde expresamente se desconoce su vigencia, como es el caso de Argentina y Colombia, y esto debido a que se considera difícil establecer responsabilidad subjetiva de los buscadores, así como la validez de las notificaciones judiciales y extrajudiciales, y los límites y limitaciones de la libertad de expresión y de la censura previa.

Nicaragua es la primera norma latinoamericana que reconoce de forma expresa el derecho al olvido digital; lo configura como un derecho del titular de solicitar a las redes sociales, navegadores y servidores a que se supriman y cancelen los datos personales.

De otro lado, México establece una discusión sobre si debe o no existir este derecho, principalmente, por la dificultad de que mediante estos mecanismos se permita la impunidad de personas responsables de actos de corrupción o se altere la memoria histórica.

Costa Rica desarrolla el derecho al olvido desde una perspectiva de conservación de datos personales, desde una prolongación excesiva que afecta a su titular, salvo disposición normativa, o que por el acuerdo de partes se haya establecido otro plazo, que exista relación continuada entre las partes o que medie interés público para conservar el dato.

Por su parte, Perú lo reconoce mediante resoluciones dictadas por la Dirección General de Protección de Datos Personales en Expediente 045-2015-JUS/DGPDP que sanciona a Google Inc., domiciliada en Estados Unidos, obligándole a desindexar información relacionada a un juicio penal cubierto por medios de comunicación, del que nunca se le encontró responsable.

El Estándar Iberoamericano de Protección de Datos Personales no lo incluye en sus recomendaciones.

La normativa ecuatoriana no hace alusión alguna a este derecho, además tampoco se ha producido un reconocimiento jurisprudencial. Sin embargo, de conformidad con el artículo 11, numeral 7, de la Constitución establece que el reconocimiento de los derechos y garantías establecidos en la Carta Magna, y en los instrumentos internacionales de derechos humanos, no excluirán los demás derechos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades, que sean necesarios para su pleno desenvolvimiento. En otras palabras, aquellos derechos que no son parte de la Constitución ni de un instrumento internacional invocable por Ecuador, pueden llegar a incorporarse a la normativa ecuatoriana en virtud de lo dicho y, además, en aplicación del principio de progresividad de derechos que consta en el artículo 11, numeral 8, CRE.

Todo esto da luces que debe reconocerse este derecho en una normativa de protección de datos personales. Lo que si debe ser claro es que, en el caso de Ecuador, por las condiciones propias de sus realidades sociales, culturales y legales, es necesario que esta decisión provenga de un tribunal constitucional que realice la debida ponderación de derechos que se presente en cada caso puesto en su conocimiento.

2. 6.5.10 Spam

En el RGPD no existe mención alguna sobre comunicaciones electrónicas no autorizadas, los Estándares Iberoamericanos de Protección de Datos Personales tampoco sugieren incorporar el *spam* en este tipo de normativas.

En el contexto latinoamericano, la legislación regula el correo no deseado o la restricción al envío masivo de mensajes, en el desarrollo de otras normativas como la que regula la sociedad de la información, por ejemplo, en Bolivia;[1852] o aquel relativo el marco civil de internet en el Brasil[1853] o desde los derechos del consumidor en Chile,[1854] como tipo penal que prohíbe el envío masivo de comunicaciones, en Costa Rica;[1855] desde la perspectiva del derecho al consumidor en México; incluso se ha configurado un tipo penal. En Perú existe una ley específica, la Ley 28493, 12 de abril del 2005, que regula el uso del correo

[1852] Presidencia del Estado Plurinacional de Bolivia, "Decreto Supremo 1793, que aprueba el Reglamento a la *Ley 164, para el Desarrollo de Tecnologías de Información y Comunicación*, 8 de agosto de 2011, Gaceta Oficial del Estado Plurinacional de Bolivia, accedido 21 de septiembre de 2017, http://www.cepb.org.bo/calypso/juridica/adjuntos/ds_1793.pdf.

[1853] Marco Civil Brasileño de Internet en Español, *Ley 12.965*, 23 de abril de 2014, que establece los principios, garantías, derechos y deberes para el uso de Internet en Brasil", Centro de Documentación e Información Edições Câmara Brasília 2015, accedido 22 de mayo de 2017, https://eva.fing.edu.uy/pluginfile.php/99128/mod_resource/content/1/marco_%20civil%20_internet.pdf.

[1854] *Ley de Protección del Consumidor, Ley 19.496*, 7 de febrero de1997, reformada por la Ley 19955, artículo único 20, D.O. 14.07.2004, 2004.

[1855] Artículo 232, Código Penal de Costa Rica.

electrónico comercial no solicitado; la Autoridad Nacional para la Innovación Gubernamental encabeza el CSIRT Panamá, mediante aviso 2014-07- Correos no deseados (*SPAM*), 15 de abril de 2014, determina criterios que deben ser aplicados por usuarios de sistema de correo electrónico para evitar *spam*. En los citados países latinoamericanos no se regula el *spam* o correo no deseado, como forma de protección del titular de dato personal.

De otro lado, Argentina, por vía judicial[1856] y mediante el *Registro Nacional "No Llame":* reconocida en la Ley 26.951, de 5 de agosto de 2014, determina la creación de un registro que protege a toda persona física o jurídica de los abusos del procedimiento de contacto, publicidad, oferta, venta y regalo de bienes o servicios no solicitados; Nicaragua en la Ley de Protección de Datos;[1857] Uruguay, mediante la Unidad Reguladora y de Control de Datos Personales de Uruguay ha dictado un informe sobre la necesidad de consentimiento informado y la posibilidad de solicitar la eliminación de listas de correos mediante denuncias a esta unidad.[1858] Es decir, estos tres países reconocen al *spam* o envío de correo masivo no deseado como parte del derecho a la protección de datos personales.

Ecuador contempla una normativa específica sobre correo no deseado en el artículo 50 de la Ley de Comercio Electrónico y Mensaje de Datos; allí determina que el envío periódico de mensajes de datos no deseados debe permitir la exclusión de las listas.

En suma, no es necesario incorporar en una normativa de protección de datos personales ecuatoriana una referencia a este derecho, pues se encuentra regulado por la citada ley. Además, pese a que algunas regulaciones lo han incluido, no es parte del contenido esencial del derecho a la protección de datos personales.

2. 6.5.11 Otros derechos

De conformidad con el estudio realizado se puede dilucidar una serie de derechos que se han agregado a los mecanismos de defensa existentes dentro de un sistema de protección de datos personales, principalmente en las regulaciones latinoamericanas.

Se destaca que los otros derechos que han tenido mayor repercusión y que incluso se encuentran reconocidos en el RGPD son parte de las sugerencias propuestas en los Estándares Iberoamericanos de Protección de Datos Personales —que se los analizará de forma individualizada en acápites posteriores—. A continuación se analizarán aquellos que pese a su importancia pueden entenderse incluidos en otros derechos y, por tanto, no marcan una independencia que justifique su incorporación en la normativa ecuatoriana de protección de datos personales.

a) Derecho de divulgación: Por el cual el órgano de control tiene la obligación de elaborar una estrategia de comunicación que permita que los ciudadanos conozcan los derechos y

[1856] Juzgado Civil y Comercial Federal 3, Secretaría 6 de la Capital Federal, 2003.
[1857] *Ley 787, Ley de Protección de Datos Personales de Nicaragua*, 29 de marzo de 2012 - vLex Global.
[1858] Unidad Reguladora y de Control de Datos Personales del Uruguay, "Esto es SPAM: informe sobre correo basura", accedido 4 de septiembre de 2017, https://datospersonales.gub.uy/inicio/institucional/noticias/esto-es-spam.

mecanismos de defensa derivados del manejo de sus datos personales, normativa prevista en Costa Rica.[1859]

b) Derecho de revocar: En Costa Rica, esta manifestación de voluntad que es parte del principio de consentimiento ha sido previsto como derecho ya que permite que el titular puede revocar el consentimiento para el tratamiento de sus datos personales.[1860]

c) Derecho a la tutela: Este derecho otorga al titular o al encargado de recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de *habeas data*.

d) Derecho a impedir suministro o a comunicar datos o de cesión: Respecto de la cesión, Perú y Uruguay reconocen un derecho que impide la cesión de datos personales a diferencia de la mayoría de legislaciones que la toman como forma de tratamiento y se contemplan como manifestación del consentimiento, postura afín a la constante en el RGPD y en los Estándares Iberoamericanos de Protección de Datos Personales, para los cuales la cesión es solo una más de las formas de tratamiento de datos personales.

e) Derecho de inclusión: Uruguay reconoce un derecho que no aparece en ninguna otra normativa latinoamericana, tampoco en el RGPD, ni en los Estándares Iberoamericanos de Protección de Datos Personales: el derecho de un titular de incorporar su información en una base de datos cuando acredite un interés fundado.

f) Principio de interés superior del niño, niña y adolescente: Es indudable que este grupo etario es el más propenso a ser víctima de transgresiones a sus derechos fundamentales debido a que se encuentra en una fase de desarrollo integral no culminada, lo que evidencia que aún no han desarrollado las capacidades, habilidades y destrezas necesarias para tomar decisiones que se entienden por adecuadas en la medida que los ayuden al ejercicio de sus libertades y que, al mismo tiempo, no signifiquen un riesgo para sí mismos. En este sentido, países como Colombia establecen una prohibición expresa a los responsables de tratamiento de tratar datos personales de niños, niñas y adolescentes. Mientras que los Estándares Iberoamericanos de Protección de Datos Personales, reconociendo la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral, consideran que debe aplicarse el principio de interés superior del niño, niña y adolescente en el tratamiento de sus datos. En ese sentido, consideran que los responsables de tratamiento públicos y privados están en la obligación de promover formación que los ayude a la generación de habilidades y destrezas, en el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto de sus datos personales. Asimismo, establece que para el tratamiento de datos personales de niñas, niños y adolescentes, el responsable obtendrá la autorización del titular de la patria potestad o tutela, conforme a las normas de capacidad de cada país, con especial relevancia respecto de la prueba de dicho consentimiento.[1861] Además este derecho subsiste aun cuando el interesado ya no sea un niño, especialmente de datos que se alojan en internet (considerando [65], RGPD).

[1859] Asamblea Legislativa de la República de Costa Rica, *Ley de Protección de la Persona frente al tratamiento de sus datos personales n.º 8968*, 7 de julio de 2011.
[1860] Ibíd.
[1861] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.

En el caso del Ecuador, la mayoría de edad se determina a los 18 años, por lo tanto los menores de tal edad son adolescentes, por ende incapaces relativos;[1862] sin embargo, otras normas les asignan capacidad de ejercicio de ciertos derechos y actos y contratos, por ejemplo el voto facultativo de los adolescentes de 16 años,[1863] o la posibilidad de realizar contratos de trabajo de los adolescentes de 15 años,[1864] o la de celebrar los actos y contratos que estén comprendidos en el objeto de una organización estudiantil, laboral, cultural, artística, ambiental, deportiva o vecinal, de las que sean personeros o legítimos representantes en el ejercicio de su derecho de asociación y cuya cuantía no exceda a dos mil dólares de los adolescentes de 16 años. [1865]

En tal sentido, la normativa de protección de datos personales puede establecer que en relación con los servicios de la sociedad de la información los adolescentes sean capaces desde los 16 años. Por tanto, las actividades de tratamiento realizadas con menores de esta edad se pueden considerar ilícitas a menos que sus padres o representantes legales hayan autorizado en su nombre; en el caso de niños menores de 12 años ni aun con autorización podrán tratarse sus datos personales.

De lo analizado, se concluye que estos nuevos derechos pueden ser parte de una normativa ecuatoriana desde la perspectiva de que son elementos que garantizan una protección de sus datos, excepto el relativo al derecho de tutela, pues este está reconocido plenamente en la Constitución ecuatoriana como derecho de tutela judicial efectiva[1866] y derecho de petición,[1867] dependiendo del ámbito judicial o administrativo de su reclamo. Asimismo, tampoco el relativo al derecho de cesión que sería perjudicial para el libre flujo información, que también es una condición necesaria en el actual desarrollo económico, social y tecnológico; el cual debe más bien regularse desde la perspectiva de tratamiento y cumplir con todos los principios y derechos que se le aplique.

2.6.5.11.1 Derecho a limitar el tratamiento

La limitación del tratamiento concebido como derecho aparece en los Estándares Iberoamericanos de Protección de Datos y se recoge en el RGPD. Su nacimiento se produce debido a los avances tecnológicos que en el estado actual permiten realizar procesamientos voluminosos de datos personales, y por ello una aproximación cada vez más invasiva de la privacidad del individuo.

De ese modo, se ha desarrollado un derecho que al mismo tiempo es una obligación por parte del responsable respecto de aplicar, desde el diseño, durante el tratamiento e incluso antes de

[1862] Artículos 21 y 1463 del Código Civil del Ecuador.
[1863] Artículo 62 de la Constitución República del Ecuador y artículo 11 de la Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador, Código de la Democracia – Loe.
[1864] Congreso Nacional del Ecuador, *Código de la Niñez y Adolescencia. Ley 100*, Registro Oficial 737, 3 de enero de 2003, artículo 65, numeral 2.
[1865] Ibíd, art. 65, num. 3.
[1866] Artículo 75, Constitución de la República del Ecuador.
[1867] Artículo 66, numeral 23, Constitución de la República del Ecuador.

recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la ley y que se limiten al mínimo de datos personales (principio de minimización de datos) y que además, se limite la accesibilidad de estos, sin la intervención del titular, a un número indeterminado de personas.[1868] De esa manera, el tratamiento de datos personales se limitará a su almacenamiento durante el período que medie entre una solicitud de rectificación u oposición hasta su resolución por el responsable, y cuando estos sean innecesarios para el responsable, pero los necesite para formular una reclamación.[1869]

Desde la normativa latinoamericana una forma de aplicación de este derecho de limitación del tratamiento se concebía desde la perspectiva del bloqueo o de la suspensión asociada al principio de cancelación de datos. Argentina, Colombia, Costa Rica, México, Nicaragua y Uruguay señalan que antes de tomar la decisión de eliminar un dato y durante el tiempo de deliberación, el dato personal debe bloquearse e informarse que no puede ser usado hasta que se disponga su eliminación definitiva.

Toma especial relevancia el caso de Colombia, país en el cual se dispone que los datos personales, salvo la información pública, no puedan estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados conforme a la presente ley.

Por su parte, el RGPD señala que esta limitación del tratamiento de los datos personales no solo debe aplicarse para el caso de cancelación, sino que el titular del dato tendrá derecho a obtener del responsable la limitación del tratamiento cuando se cumplan alguna de las siguientes condiciones:

a) que se haya impugnado la exactitud del dato;

b) que se haya impugnado la ilicitud del dato;

c) que se haya impugnado la necesidad de conservación del dato; es decir, el responsable ya no necesita los datos personales para los fines del tratamiento, pero en cambio el interesado los necesita para formular acciones o para la defensa de reclamaciones;

d) que se haya impugnado por motivos legítimos.

En todos estos casos, incluidos el de solicitud de eliminación, se verificará, en un plazo razonable, el fundamento de la petición realizada y se procederá a efectuar mecanismos que garanticen la citada limitación, por ejemplo los siguientes: "trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, impedir el acceso de usuarios a los datos personales seleccionados, retirar temporalmente los datos publicados de un sitio internet"[1870] y en ficheros automatizados, a través de medios técnicos que impidan operaciones de tratamiento.

[1868] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1869] Ibíd.
[1870] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.

Finalmente, para que el responsable pueda superar la limitación impuesta por el interesado titular de la data, y pueda seguir tratando datos personales es necesario el consentimiento del interesado; o la necesidad de habilitar el tratamiento en razón del ejercicio o la defensa de los interesados; o la protección de los derechos de otra persona física o jurídica; o por razones de interés público.

La propuesta normativa que recoge este derecho sería la siguiente:

> **Artículo 29.- Derecho a la limitación del tratamiento.-** El titular tendrá derecho a que se use el mínimo de sus datos personales en el tratamiento efectuado por responsables o encargados del tratamiento datos personales; a que sus datos personales no se encuentren disponibles en internet u otros medios de comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido a los titulares o a los autorizados por razones de interés público; a que el tratamiento de datos personales se limite al período que medie entre una solicitud de revisión de juridicidad, lealtad, transparencia, legitimidad, acceso, eliminación, rectificación y actualización, oposición, anulación, portabilidad, limitación del tratamiento, a no ser objeto de una decisión basada únicamente en valoraciones automatizadas; hasta su resolución por el responsable o encargado del tratamiento de datos personales.
>
> De existir negativa por parte del responsable o encargado del tratamiento de datos personales, y el titular recurra de dicha decisión ante la Autoridad de Protección de Datos Personales, esta limitación se extenderá hasta la resolución del procedimiento administrativo.
>
> Que el responsable del tratamiento conserve únicamente los datos personales que sean necesarios para la formulación de un reclamo, una vez cumplido el plazo o condición del tratamiento.

2. 6.5.11.2 Derecho a la portabilidad

El derecho de portabilidad aparece únicamente en la legislación mexicana, en los Estándares Iberoamericanos de Protección de Datos Personales y en el RGPD. Estas tres referencias lo conciben como un derecho a recibir una copia, en formato electrónico estructurado, de uso común, de lectura mecánica y con formato interoperable, los datos personales que un titular ha facilitado a un responsable del tratamiento o para transmitirlos a otro responsable del tratamiento directamente, luego de lo cual procederá a su eliminación a menos que exista consentimiento del titular o condición legal que lo impida.

La normativa mexicana señala que solo procede la portabilidad cuando el tratamiento ha sido realizado por vía electrónica,[1871] o conforme sugiere el RGPD y el Estándar Iberoamericano de Protección de Datos Personales, en un formato que permita seguir utilizándolos;[1872] esto es por medios automatizados que no solo permitan su uso, sino también su transferencia directa.

[1871] Ibíd.
[1872] Congreso General de los Estados Unidos Mexicanos, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*.

El número de veces que puede solicitarse este derecho y los costos para su entrega y transferencia no podrán imputarse al titular a menos que sobrepase un uso legítimo.

Se destaca que el derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros, ni aun cuando se refiera a un conjunto de datos personales determinado que concierna a más de un interesado.[1873] Por ello, puede ser aplicado siempre que no se menoscabe el derecho de cancelación, el derecho al olvido y el de limitaciones al tratamiento. En particular no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato.[1874]

Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente provenga de la personalización, recomendación, categorización o creación de perfiles.[1875]

El derecho de portabilidad para su aplicación requiere del consentimiento explícito para uno o varios fines específicos del titular del dato, incluidas categorías especiales de datos como las relativas al origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical. Asimismo, el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física únicamente si la ley lo permite, o si requieran para el mantenimiento de una relación o de una ejecución contractual, incluida la fase precontractual.

No será posible el cumplimiento del derecho de portabilidad cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato, el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público, sea necesario para el ejercicio de poderes públicos conferidos al responsable del tratamiento, o el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable.

En tal sentido, se prevé la siguiente formulación de artículo:

> **Artículo 27.- Derecho a la portabilidad.-** El titular tiene derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; y/o transmitirlos a otros responsables.
>
> El titular podrá solicitar la transferencia o comunicación de sus datos personales a otro responsable del tratamiento. Luego de completada la transferencia, el responsable que transfiere dichos datos procederá a su eliminación.
>
> Para que proceda el derecho a la portabilidad de datos es necesario que se produzca al menos una de las siguientes condiciones:

[1873] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.
[1874] Ibíd.
[1875] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.

a) Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos, la transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible;

b) Que el tratamiento se efectúe por medios automatizados;

c) Que se trate de un volumen relevante de datos personales; o,

d) Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos personales, o del titular en el ámbito del derecho laboral y seguridad social.

Está transferencia o comunicación debe ser económica y financieramente eficiente, expedita, efectiva y sin trabas.

No procederá este Derecho cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable del tratamiento de datos personales con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

2. 6.5.11.3 Derecho de transparencia

Como se analizó en el ítem 5.9.1, denominado del deber de información a la transparencia, además de ser un principio, se considera un derecho por el cual se establece la facultad que tienen los titulares de exigir que la información, comunicación y modalidades de ejercicio de los derechos del interesado se realice con transparencia y lealtad, de modo que el responsable tome medidas oportunas para facilitar al interesado toda información que permita el ejercicio de sus derechos, en el momento de la recogida de datos, para la obtención del consentimiento, en cualquier momento cuando no se haya obtenido el consentimiento directamente del interesado.[1876]

Solo en una interrelación transparente y leal entre responsables y titulares de los datos se pueden construir relaciones sanas que busquen mutuos beneficios, que les favorezcan positivamente y generen relaciones de confianza y credibilidad.

Además, la transparencia es un derecho aplicable a toda información dirigida al público en general, ya que permite que la sociedad acceda a información y comunicaciones que faciliten el ejercicio de sus derechos subjetivos, principalmente, en su relación con el tratamiento de datos personales que los responsables se encuentran implementando; así, garantizar una cultura de protección de los datos personales. En este sentido, de los países latinoamericanos únicamente México determina que cuando un documento o expediente contenga partes o secciones reservadas o confidenciales, los sujetos obligados a efectos de atender una solicitud de información deberán elaborar una versión pública en la que se transcriban las partes o

[1876] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.

secciones clasificadas, indicando su contenido de manera genérica, fundando y motivando su clasificación.[1877]

Asimismo, la Asamblea General de las Naciones Unidas, en su resolución A/C.3/68/L.45/Rev.1 sobre el Derecho a la Privacidad en la Era Digital, señala que los Estados tienen la obligación de establecer o mantener mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia.[1878] En este sentido, la transparencia también es una obligación estatal, ya que como garante debe establecer un entorno que permita la realización de los derechos de sus ciudadanos.

Todas esas aristas conforman el derecho a la transparencia, desde la prerrogativa del ciudadano, en sus cuestiones particulares, de la sociedad cuando se dispone de información accesible al público en general, así como del Estado como garante de los derechos de sus ciudadanos. Por lo expuesto, se establece la siguiente propuesta de normativa:

> **Artículo 21.- Derecho a la lealtad, transparencia e información.-** El titular de datos personales tiene derecho a ser informado de forma leal y transparente por cualquier medio sobre:
>
> a) Los fines del tratamiento;
>
> b) Base legal para el tratamiento;
>
> c) Tipos de tratamiento;
>
> d) Tiempo de conservación;
>
> e) La existencia de una base de datos en donde consten sus datos personales;
>
> f) El origen de los datos personales cuando no se hayan obtenido directamente del titular;
>
> g) Otras finalidades y tratamientos ulteriores;
>
> h) Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluye: dirección de domicilio legal, número de teléfono y correo electrónico;
>
> i) Identidad y datos de contacto del delegado de protección de datos personales, que incluye: dirección domiciliaria, teléfono y correo electrónico;
>
> j) Las transferencias o comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de las mismas;
>
> k) Carácter obligatorio o facultativo de la respuesta y las consecuencias de proporcionar o no sus datos personales;

[1877] Artículo 118, *Ley General de Transparencia y Acceso a la Información Pública», Corpus iuris en materia de protección de datos personales*, 5 de abril de 2015, http://corpusiurispdp.inai.org.mx/iberoamericano/Instrumentos/LGTAIP.pdf.

[1878] Asamblea General de las Naciones Unidas, *Resolución A/C.3/68/L.45/Rev.1 sobre el Derecho a la Privacidad en la Era Digital.*

l) El efecto de suministrar datos personales erróneos o inexactos;

m) La posibilidad de revocar el consentimiento;

n) La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas;

o) Los mecanismos para hacer efectivo su derecho a la portabilidad, cuando el titular lo solicite;

p) Donde y como realizar sus reclamos ante el responsable del tratamiento de datos personales y la Autoridad de Protección de Datos Personales; y,

q) La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles.

En el caso que los datos fueran obtenidos directamente del titular, la información deberá ser comunicada de forma previa a éste es decir, en el momento mismo de la recogida del dato personal.

Excepcionalmente, el titular deberá ser informado de forma posterior, dentro del mes siguiente, cuando los datos personales no se obtuvieren de forma directa; expresa; transparente; inteligible; concisa; precisa; sin barreras técnicas; e, inequívoca.

Con el objeto de que pueda autorizar el tratamiento, transferencia o comunicación de sus datos personales, esta información deberá ser proporcionada al titular de forma accesible por cualquier medio, incluidas políticas de protección de datos personales; gratuitos; suficientes; disponibles de forma permanente y redactarse en un lenguaje claro; sencillo; y, de fácil comprensión incluso cuando se trate de contratación electrónica.

En el caso de productos o servicios dirigidos, utilizados o que pudieran ser utilizados por niñas, niños y adolescentes, la información a la que hace referencia el presente artículo será proporcionada a su representante legal conforme a lo dispuesto en el inciso precedente.

2.7 Restricciones a las obligaciones, los derechos y los principios

El RGPD establece limitaciones a las obligaciones, los principios y derechos que son parte del derecho a la protección de datos personales. Esto mediante medidas legislativas que respetan en lo esencial los derechos y libertades fundamentales y se constituyan en la medida en que sean necesarias y proporcionadas en una sociedad democrática para salvaguardar: la seguridad del Estado, la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano; la defensa; la prevención, investigación, detección o enjuiciamiento o ejecución de infracciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención; otros objetivos importantes de interés público general, en particular un interés económico o financiero, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social. Asimismo, para salvaguardar la llevanza de registros públicos por razones

de interés público general, el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios, o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios, la protección de la independencia judicial y de los procedimientos judiciales; la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas. También, una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública; la protección del interesado o de los derechos y libertades de otros; la ejecución de demandas civiles, conforme consta en el artículo 23 y en el considerando (73) del RGPD.

Esta lista refleja la necesidad de normativa específica que permita establecer regímenes específicos y especializados de protección, para los cuales se justifica un régimen acotado que consiste en aquellos elementos mínimos o de contenido esencial del derecho a la protección de datos personales.

La OEA en el principio 12 establece la necesidad de que se publicite las excepciones establecidas por autoridades de control, respecto de regímenes reducidos justificados relacionados con la soberanía nacional, la seguridad interna o externa, el combate con la criminalidad, el orden público, la salud pública o la moralidad, el cumplimiento de normativas u otras prerrogativas de orden público.[1879]

2.8 Procedimiento administrativo

El sistema de protección de datos personales tiene tres regímenes de tutela del derecho: a) El primero es una tutela básica, ante juzgados ordinarios, no existe órgano de control y opera para el reconocimiento de una omisión en el cuidado de los datos como el caso de Guatemala y El Salvador. b) El segundo sistema es el de acciones directas y administrativas, esto es exigibles directamente al responsable de la base de datos, o por intermedio de una autoridad de control estatal que proteja el derecho; estas acciones operan en una esfera preventiva y reactiva, intentando desarrollar actividades de vigilancia, control para evitar que el daño se produzca, así como sancionar las infracciones que hayan transgredido derechos y hayan causado daño.[1880] Los Estándares Iberoamericanos de Protección de Datos establecen como

[1879] Asamblea General OEA, 86 Período Ordinario de Sesiones, CJI/doc. 474/15 rev.2 Río de Janeiro, Brasil, 26 marzo 2015, *Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales*, http://www.oas.org/es/sla/ddi/docs/cji-doc_474-15_rev2.pdf.

[1880] El RGPD establece varios procedimientos que permiten la solicitud o reclamación por parte del titular de los datos personales:

a) Mecanismos para solicitar acceso, rectificación, supresión u oposición directamente al responsable o encargado del tratamiento: Mecanismo por el cual el titular puede obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición.

b) Derecho a presentar una reclamación ante una autoridad de control única: Por la cual, el titular tiene derecho a presentar una reclamación ante una autoridad de control con la finalidad de que pueda impedir que se siga produciendo la violación a la normativa sobre tratamiento de datos, y el responsable rectifique su actuación. Esta reclamación procede sin perjuicio de cualquier otro recurso administrativo o acción judicial que se haya presentado.

c) Derecho a la tutela judicial efectiva contra una autoridad de control: Por el cual, un interesado puede accionar esta tutela una vez que no haya sido contestada o se haya dictado una decisión jurídicamente vinculante que haya negado o desestimado total o parcialmente una reclamación previa, presentada ante una autoridad de

precepto que las decisiones de las autoridades de control únicamente estarán sujetas al control jurisdiccional.[1881] c) Finalmente, está el sistema desarrollado en Latinoamérica que es un híbrido, puesto que es posible realizar reclamaciones ante los responsables de forma directa,[1882] ante una autoridad de control[1883] y, al mismo tiempo, presentar garantías constitucionales de tutela como el *habeas data* de categoría constitucional[1884] o de justicia ordinaria.[1885] Sin embargo, las acciones constitucionales deben verse como un sistema de clausura, ya que solo puede usarse cuando hay un inminente peligro o cuando se ha producido una transgresión específica, y en ese sentido solo opera cuando ya se ha producido el daño. Por eso, la garantía del *habeas data* constituye un mecanismo reactivo para defender derechos como la intimidad, protección de datos personales, honor imagen, entre otros, quedándose de lado todo el sistema de prevención que permite a los responsables de tratamiento organizarse con la finalidad de cumplir con los principios, obligaciones,

---

control. La presentación de la tutela judicial efectiva puede realizarse sin perjuicio de que se haya interpuesto otro recurso administrativo o extrajudicial.

d) Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento: Por el cual, el titular establece el derecho a la tutela judicial efectiva contra el responsable o encargado del tratamiento, para que este, por sí mismo permita el acceso, modifique, suprima, o en general adapte su comportamiento a las disposiciones contenidas en el RGPD; sin perjuicio del interesado de iniciar las acciones tendientes a solicitar la indemnización por daños y perjuicios previsto en el artículo 82 del RGPD. Todo interesado tendrá derecho a presentar tutela judicial efectiva aunque se haya interpuesto otro recurso administrativo o extrajudicial disponible, incluido el derecho a presentar una reclamación ante una autoridad de control previsto en el artículo 77 del RGPD.

e) Derecho a indemnización y responsabilidad: El interesado puede solicitar al responsable la indemnización de los daños y perjuicios causados por las transgresiones a los derechos del titular por el indebido tratamiento de sus datos personales. Todos los derechos reconocidos en el RGPD, que debido a su vulneración han producido daños materiales o inmateriales a su titular y que puedan ser avaluados a título de indemnización. Tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

[1881] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.

[1882] Acciones directas contra el responsable de la base de datos: Países que basan su sistema de protección en la intimidad y la privacidad o con leyes sectoriales limitadas al ámbito público: El Salvador. Acciones directas contra el responsable de la base de datos contenidos en Leyes de Protección de Datos Personales: Argentina, Colombia, Costa Rica, México, Nicaragua, República Dominicana y Uruguay.

[1883] Acciones ante autoridades administrativas competentes en protección de datos personales: Costa Rica, Perú, Nicaragua, México (tanto en la normativa de protección de datos personales para el sector privado, como para el público). Jamaica y Puerto Rico (acción administrativa de privacidad). Acciones administrativas en países que basan su sistema de protección en la intimidad y la privacidad o con leyes sectoriales limitadas al ámbito público o específicos: El Salvador, Brasil (limitadas a relaciones contractuales de servicios de telecomunicaciones, Marco Civil de Internet) y Chile.

[1884] Garantía constitucional (*habeas data*): Brasil (1988), Paraguay (1992), Perú (1993), Ecuador (1996), Venezuela (1999), Panamá (2002), Honduras (2003), República Dominicana (2010) y Nicaragua (2014). Otras acciones constitucionales: Se anota que en otros países no se reconoce el *habeas data*; en su lugar existen acciones constitucionales tradicionales como la tutela y el amparo que incluyen en ellas al *habeas data*. Colombia (1991), mediante la acción de tutela constitucional; Argentina, mediante la acción de amparo (subtipo de amparo constitucional o *habeas data* constitucional) (1994); y México por medio de la Ley de Amparo, Reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos, cuyas últimas modificaciones corresponden al 17 de junio de 2016 que regula el Juicio de Amparo que procede sobre derechos constitucionales como el de protección de datos personales (art. 16 de la Constitución citada). Bolivia consagra en la Constitución la acción denominada de protección de la privacidad.

[1885] Acción de protección de los datos personales o de *habeas data* legal (acción judicial): Argentina, Uruguay, Perú (agotamiento de vía procede la acción contencioso administrativa) y República Dominicana.

responsabilidades y derechos con la finalidad de evitar causar daño y, en consecuencia, evitar la comisión de infracciones y la atribución de sanciones.

Por su parte el RGPD señala que cuando no existencia una decisión de adecuación en una trasferencia internacional de datos, el responsable o el encargado del tratamiento debe tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas, entre las cuales consta la de establecer derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización.

Los Estándares Iberoamericanos de Protección de Datos Personales establecen criterios que deben ser recogidos para garantizar que los procedimientos directos, aquellos que se interponen al responsable de la base de datos y administrativos, por los cuales se acude a la autoridad de control; en otras palabras, que sean medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad.[1886]

Por su parte, Ecuador es uno de los países en los cuales la forma de tutela del derecho a la protección de datos personales está únicamente dirigida a la garantía constitucional de *habeas data*.

Esta acción no debe ser única, ya que Ecuador debe optar por un sistema híbrido: que una norma habilite otras formas de reclamación, dado que un sistema exclusivamente anclado al *habeas data* no ofrece un sistema integral del derecho por ser un mecanismo reactivo, utilizable cuando el daño está por ocurrir o ya se ha producido. La realidad internacional demuestra que es preferible afianzar un sistema en el cual se evite la transgresión de los derechos mediante mecanismos de control y vigilancia, en los que además se pueda articular directamente con el responsable de primera mano una solución, o se arbitre soluciones por parte de autoridades de control que prevean la existencia de medidas que evitan mayores daños. Finalmente, acciones o tutelas administrativas o judiciales, incluida la constitucional de *habeas data*, que se usen cuando sea evidente la existencia de un daño, por ende es necesario verificar si las actuaciones de responsables constituyen infracciones que deben ser sancionadas con la correspondiente medida, multa e indemnización que corresponda.

Por eso, en el propio texto de la propuesta normativa se debe incluir, medios y procedimientos sencillos, expeditos, accesibles y gratuitos para que el titular pueda reclamar directamente al responsable, especialmente en lo que se refiere a derechos de acceso, rectificación, cancelación, oposición y portabilidad, sin perjuicio de que pueda activar la vía administrativa, judicial o constitucional de considerarlo pertinente, sobre todo en aquellos casos en los cuales exista una negativa del responsable, o ante la falta de respuesta de este ante la autoridad de control y, en su caso, ante instancias judiciales.[1887]

De otro lado, la normativa ecuatoriana faculta mecanismos de tutela administrativa, dado que el artículo 11, numeral 3 de la Constitución de la República del Ecuador establece que los derechos y garantías establecidos en dicho cuerpo normativo y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de

[1886] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1887] Ibíd.

parte. En el mismo sentido, el artículo 66, numeral 23 de la norma *ibídem* reconoce el derecho a dirigir quejas y peticiones individuales y colectivas a las autoridades y a recibir atención o respuestas motivadas.

Los estándares sugieren que el procedimiento administrativo que provee cada Estado debe establecer los requerimientos, plazos, términos y condiciones en que los titulares podrán ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad,[1888] lo que en el caso del Ecuador podría estar subsanado debido a que se cuenta con una normativa de aplicación general que cubre estos requisitos, la cual se analizará a continuación.

Ahora bien, el Segundo Suplemento del Registro Oficial 31, 7 de julio de 2017, entró en vigencia el Código Orgánico Administrativo (COA) que en el artículo 42 al referirse al ámbito de aplicación material en su numeral 1 dispone: "Art. 42.- Ámbito material.- El presente Código se aplicará en: [...] 1. La relación jurídico administrativa entre las personas y las administraciones públicas".

Por otra parte, el artículo 134 del COA determina que las reglas contenidas en el procedimiento administrativo común aplican a los reclamos administrativos, así como para el ejercicio de la potestad sancionadora.

Bajo los antecedentes expuestos todo procedimiento administrativo que refiera a la relación jurídico-administrativa entre las personas y las administraciones públicas que incluyen las actividades formal y materialmente administrativas de la función Ejecutiva y funciones materialmente administrativas de las funciones Legislativa, Electoral, Judicial y de la función de Participación Ciudadana y Control Social se sujetarán a las disposiciones que rigen al procedimiento común y procedimiento especial sancionatorio que se encuentra establecido en el Código Orgánico Administrativo.

El COA establece para el procedimiento común las siguientes etapas secuenciales:

1. *Legitimación*. El artículo 149 del Código Orgánico Administrativo establece que estarán legitimados para iniciar el procedimiento administrativo:

    a. Quien promueva el procedimiento como titular de derechos o intereses legítimos individuales o colectivos;

    b. Quien invoque derechos subjetivos o acredite intereses legítimos, individuales o colectivos, que puedan resultar afectados por la decisión que se adopte en el procedimiento;

    c. Quien acredite ser titular de derechos o intereses legítimos de las asociaciones, organizaciones, los grupos afectados, uniones sin personalidad, patrimonios independientes o autónomos y comparezca al procedimiento antes de la adopción de la resolución.

    El procedimiento administrativo puede iniciar de oficio o a petición de parte.

[1888] Ibíd.

2. *Medidas Cautelares*. El Código Orgánico Administrativo faculta al órgano instructor a dictar medidas cautelares de oficio o a petición de parte, pudiéndose dictar las siguientes:

    a. Secuestro;

    b. Retención;

    c. Prohibición de enajenar;

    d. Clausura de establecimientos;

    e. Suspensión de la actividad;

    f. Retiro de productos, documentos u otros bienes;

    g. Desalojo de personas;

    h. Limitaciones o restricciones de acceso;

    i. Otras previstas en la ley.

    En todos los casos las medidas cautelares deben ser razonables, proporcionales y afectar lo menos posible al ejercicio de los derechos de las personas

3. *Prueba*. Atendiendo al derecho al debido proceso reconocido en el artículo 76 de la Constitución de la República del Ecuador, todo administrado tiene derecho a ser oído, con las debidas garantías y dentro de un plazo razonable por un juez o tribunal competente e imparcial; es decir, a ofrecer, producir y controlar la prueba sustanciada dentro del correspondiente procedimiento administrativo.

4. *Resolución*._Es el acto administrativo por medio del cual se pone fin al procedimiento administrativo.

5. *Notificación*._Conforme dispone el artículo 164 del COA, la notificación constituye el acto por medio del cual se da a conocer a la parte interesada o a un conjunto indeterminado de personas, el contenido de un acto administrativo para que las personas interesadas estén en condiciones de ejercer sus derechos.

El artículo 77 del Reglamento Europeo establece que, sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe dicho reglamento.

Particular que se ajusta al presupuesto referido tanto en la Constitución de la República del Ecuador, que atiende al derecho de petición a favor del administrado, como al procedimiento contemplado el Código Orgánico Administrativo, el cual ha sido referido de forma sumaria en líneas precedentes.

En cuanto al procedimiento administrativo sancionatorio, el Código Orgánico Administrativo establece una serie de garantías relacionadas con el ejercicio de la potestad sancionatoria en materia administrativa, la cual constituye una manifestación del *Ius puniendi* del Estado, expresión latina utilizada para referirse a la facultad sancionatoria del Estado, que se encuentra constreñida a los principios jurídicos generales que limitan su ejercicio, entre los cuales están los de legalidad y tipicidad, proporcionalidad, concurrencia de sanciones y el de irretroactividad.

Las sanciones administrativas suelen tener la misma o similar naturaleza a las penales y, al igual que estas, son una expresión del poder punitivo del Estado. Unas y otras implican menoscabo, privación o alteración de los derechos de las personas, como consecuencia de una conducta ilícita. Por lo tanto, es indispensable que la norma punitiva, ya sea penal o administrativa, exista y sea reconocida o pueda serlo, antes de que tenga lugar el hecho y omisión que la transgredan y que se pretende sancionar.

En función de dicho presupuesto, el Código Orgánico Administrativo contempla las siguientes garantías a favor del administrado en función del ejercicio de la potestad sancionadora:

1. Se dispondrá la debida separación entre la función instructora y la sancionadora, que corresponderá a servidores públicos distintos;

2. En ningún caso se impondrá una sanción sin que se haya tramitado el necesario procedimiento;

3. Se deberá notificar al presunto responsable con los hechos que se le imputen, de las infracciones que tales hechos puedan constituir y de las sanciones que se le pueda imponer;

4. Presunción de inocencia.

El procedimiento sancionatorio contempla, además, las siguientes etapas preclusivas:

1. *Acto de inicio*.- En el cual se hará constar la identificación de la persona o personas presuntamente responsables, la relación de los hechos que motivan el inicio del procedimiento; detalle de los documentos o informes que sirven de sustento; y determinación del órgano competente para resolver el caso.

2. *Notificación del acto de inicio*.- Consiste en dar a conocer al presunto infractor del acto de inicio con el objeto de dar la posibilidad de que ejerza su legítimo derecho a la defensa.

3. *Actuaciones de instrucción*.- En esta etapa el presunto infractor podrá alegar, aportar documentos o información que estime conveniente y solicitar la práctica de las diligencias probatorias que considera convenientes.

4. *Prueba*.- En el ejercicio de la potestad sancionadora se invierte la carga de la prueba a favor del administrado, siendo la administración la que, en aplicación de los principios de impulso de oficio, verdad material e informalismo que rige al procedimiento administrativo, debe agotar los recursos necesarios para establecer la existencia de la infracción por la cual se busca sancionar al presunto infractor.

5. *Resolución.*- Acto administrativo mediante el cual se da por terminado el procedimiento administrativo.

Tanto para el procedimiento administrativo común como en el procedimiento administrativo sancionador, el Código Orgánico Administrativo contempla un régimen impugnatorio en vía administrativa sea mediante el uso del recurso de apelación o el extraordinario de revisión, sin perjuicio de que las resoluciones adoptadas por la Administración Pública puedan ser conocidas y resueltas por la Función Jurisdiccional. Dicho presupuesto se alinea con la disposición contenida en el artículo 78 del Reglamento (UE) 2016/679 del Parlamento Europeo, el cual determina que, sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.

Asimismo, el artículo 78, numeral 2) del Reglamento antes referido establece que todo interesado tendrá derecho a la tutela judicial efectiva en caso de que la autoridad de control que sea competente, en concordancia con los artículos 55 y 56 del reglamento, no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o resultado de la reclamación presentada en virtud del artículo 77.

En ese sentido, el artículo 173 de la Constitución de la República del Ecuador establece que los actos administrativos de cualquier autoridad del Estado podrán ser impugnados, tanto en la vía administrativa como ante los correspondientes órganos de la Función Judicial.

El artículo 168 de la norma *ibídem* establece que la administración de justicia se rige, entre otros principios, en el de unidad jurisdiccional, el cual determina que ninguna autoridad de las demás funciones del Estado podrá desempeñar funciones de administración de justicia ordinaria, sin perjuicio de las potestades jurisdiccionales reconocidas por la Constitución.

El ejercicio de las atribuciones de inspección, supervisión y control y el de ejercer poder coercitivo acerca de la posibilidad de imponer sanciones de índole administrativa en caso de verificarse la concreción de una infracción de esa índole; no faculta al ente de control a establecer mecanismos de reparación integral ante el posible perjuicio que derive de un acto u omisión que afecte el ejercicio de un derecho ciudadano, pretensión que en observancia al principio de unidad jurisdiccional debe ser canalizado mediante los órganos que ejercen formal y materialmente funciones jurisdiccionales.

De lo previsto, se proponen los siguientes textos:

> **Artículo 69.- Queja directa del titular del dato personal al responsable del tratamiento de datos personales.-** El titular de los datos personales podrá, en cualquier momento, de forma gratuita y por medios físicos o digitales puestos a su disposición por parte del responsable del tratamiento de los datos personales, presentar quejas sobre el contenido de los derechos, principios y obligaciones para hacer efectivas de forma directa sus peticiones, en especial aquellas relacionadas al acceso, rectificación o actualización, eliminación, oposición, limitaciones al tratamiento, portabilidad, notificaciones sobre violaciones a la seguridad, transferencia internacional a terceros países, entre otros.

Presentada la queja ante el responsable, este contará con un plazo de cinco días para contestar y notificar en debida forma sobre su respuesta afirmativa o negativa, y ejecutar lo que se le haya solicitado.

2.9 Institucionalidad de protección: Institucionalidad especializada para regulación, prevención, control y sanción

El RGPD y los Estándares de Protección de Datos Personales, así como una parte de la normativa latinoamericana, coinciden en los criterios indispensables para la creación de una o varias autoridades de control de protección de los datos personales que garanticen los derechos y garantías que son parte del sistema de protección de los titulares de los datos personales y la regulación del libre flujo informacional.

Esta institucionalidad deberá contar con atribuciones, competencias, suficientes poderes de investigación, supervisión, resolución, promoción y sanción, así como con suficientes recursos económicos, humanos y técnicos[1889] que permitan la vigencia de los derechos, deberes y obligaciones descritas en la ley, prevenir posibles transgresiones, vigilar y sancionar su incumplimiento y viabilizar un trabajo imparcial y técnico.

El criterio más importante que debe cumplir cualquier autoridad de control es la independencia que les permita ejercer sus funciones sin influencia externa y estar a resguardo de toda influencia externa, ejercida directa o indirectamente, que pueda orientar sus decisiones.[1890] Es preocupación de las Naciones Unidas también el tema de la independencia, de tal forma en sus recomendaciones establecen que debe mantenerse mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado.[1891]

La independencia debe ser entendida en las siguientes dimensiones: a) en el desempeño de sus funciones; b) en el ejercicio de los poderes de investigación, correctivos, de autorización y consultivos; c) de cada miembro o miembros de la autoridad de control, no se solicitará ni admitirá ninguna forma de instrucción, en el desempeño de sus funciones y en el ejercicio de sus poderes públicos; d) el miembro o los miembros de cada autoridad de control se abstendrán de realizar cualquier acción pública o privada que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no; e) independencia de recursos humanos, técnicos y financieros, sin que esto signifique que puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial; e) libertad en el escogimiento del personal.

Ahora bien, del análisis de las normativas latinoamericanas también se encuentra que varios países tienen instituciones autónomas e independientes cuya competencia exclusiva es la protección de datos personales, tales como: Argentina, mediante la Dirección Nacional de Protección de Datos Personales; Costa Rica y la Agencia de protección de Datos de los

[1889] Ibíd.
[1890] Tribunal de Justicia de la Unión Europea, "Asunto C518/07, en el caso Comisión/Alemania", 2010, accedido 13 de octubre de 2018, http://curia.europa.eu/juris/liste.jsf?language=es&num=C-518/07.
[1891] Asamblea General de las Naciones Unidas, "Resolución A/C.3/68/L.45/Rev.1 sobre el Derecho a la Privacidad en la Era Digital".

Habitantes; Nicaragua, mediante la Dirección de Protección de Datos Personales, adscrita al Ministerio de Hacienda y Crédito Público. Uruguay, por intermedio de la Unidad Reguladora y de Control de Datos Personales, que es parte de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic).

Sin embargo, México ha asignado esta competencia al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), organismo que se dedica, tanto a la protección del dato público como del dato personal.

Existen países que atribuyen la competencia de proteger los datos personales a instituciones que tienen otras competencias como es el caso de: Colombia, por medio de la Superintendencia de Industria y Comercio (SIC); Perú, mediante la Autoridad Nacional de Protección de Datos Personales, dependiente de la Dirección Nacional de Justicia del Ministerio de Justicia. Estos casos son de los más cuestionados porque no garantizan un nivel de independencia e imparcialidad estructural debido a que estas instituciones tienen otras competencias que suelen ser prioritarias en comparación con la relativa a la protección de datos personales y el libre flujo de información.

Finalmente, Ecuador y Panamá no cuentan ni con instituciones ni competencias atribuidas a las existentes.

El artículo 11, numeral 3 de la Constitución de la República del Ecuador determina que los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte.

El numeral 9 del artículo previamente referido determina que el más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución; así el artículo 66, numeral 19) de la Constitución reconoce y garantiza a las personas, entre otros derechos, el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter.

Tanto las personas naturales como jurídicas, sean estas de naturaleza pública o privada, manejan información que es necesaria para el cumplimiento de sus fines y objetivos. El tránsito de datos mediante los diversos organismos que conforman el sector público, exige la creación de una entidad que goce del suficiente nivel de autonomía e independencia que posibilite el efectivo ejercicio de las funciones de inspección, supervisión y control sobre el uso de la información; por eso es necesario dotar a dicho ente de las siguientes características:

a) Personalidad jurídica.

b) Mecanismos complejos de designación de sus titulares.

c) Ausencia de remoción gubernamental discrecional. El RGPD y los Estándares Iberoamericanos de Protección de Datos Personales determinan que únicamente podrán ser

removidos por causales graves establecidas en la ley, conforme a las reglas del debido proceso.[1892]

d) Una mayor duración del mandato y su limitada renovación.

e) Singulares condiciones personales y profesionales requeridas para los cargos directivos. Además del RGPD, los Estándares Iberoamericanos de Protección de Datos Personales coinciden en que el miembro o los miembros de los órganos de dirección de las autoridades de control deberán contar con la experiencia y aptitudes, en particular respecto al ámbito de protección de datos personales, necesarios para el cumplimiento de sus funciones y el ejercicio de sus potestades. Se nombrarán mediante un procedimiento transparente en virtud de la ley.[1893]

f) Cierta potestad de auto-organización desvinculada de la que confiere el gobierno a las restantes administraciones públicas y selección de su personal.

g) Autonomía presupuestaria y patrimonial.

El reconocimiento constitucional o legal de la entidad le dota de un marco de jerarquía y perdurabilidad, lo cual constituye una primera garantía institucional, al nacer del consenso de los representantes del pueblo ante el poder constituyente o legislativo. Los organismos independientes se caracterizan tanto por la competencia de sus integrantes como por el contexto de selección y destitución de los mismos, la inamovilidad discrecional y estabilidad otorga mayores niveles de independencia.

La profesionalización tiende a inspirar el nivel de confianza requerido por la sociedad dentro de los procedimientos de control, por lo que la posibilidad de que el controlado imponga al controlante el personal que llevará a cabo las funciones de inspección, vigilancia y control transforma al ejercicio de la función en ineficaz sobre la protección misma del ejercicio del derecho que se busca precautelar, y de esa forma atenta al interés público que se busca proteger.

Los modelos de organización del Estado incorporan las figuras de desconcentración y descentralización, las cuales se diferencian en su margen de autonomía e independencia funcional. Es claro, entonces, que los entes de control deben ostentar el mayor nivel de independencia e imparcialidad reconocido en el ordenamiento jurídico para el ejercicio de las atribuciones y responsabilidades que le son encomendadas de acuerdo con la Constitución y la ley.

La tarea, entonces, se centra en identificar una figura jurídica que permita cumplir con los estándares de independencia e imparcialidad requeridos, para lo cual es preciso referirse al modelo de organización política y administrativa propuesto en la Constitución de la República del Ecuador del año 2008. Allí se incorporó un diseño democrático de división de poderes en la que se identifica a las funciones Ejecutiva, Legislativa, Judicial, Electoral, y de Transparencia y Control Social.

[1892] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.
[1893] Ibíd.

El artículo 204 de la Constitución de la República del Ecuador, al referirse a la Función de Transparencia y Control Social, determina que esta promoverá e impulsará el control de las entidades y organismos del sector público, y de las personas naturales o jurídicas del sector privado que presten servicios o desarrollen actividades de interés público y protegerá el ejercicio y cumplimiento de los derechos reconocidos en la Constitución y la ley.

Entre las instituciones que forman parte de la Función de Transparencia y Control Social, se encuentran las superintendencias, las que según lo dispuesto en el artículo 213 de la Constitución de la República del Ecuador son organismos técnicos de vigilancia, autoría, intervención y control de las actividades económicas, sociales y ambientales, y de los servicios que prestan las entidades públicas y privadas, con el propósito de que estas actividades y servicios se sujeten al ordenamiento jurídico y atiendan al interés general.

Bajo dicho presupuesto, en primera instancia, cabe analizar si el ámbito material de aplicación fijado en el artículo 213 de la Constitución sirve de base para la creación de un ente de supervisión, vigilancia y control del ejercicio del derecho a la protección de datos personales, para lo cual habrá que establecer si el nivel de incidencia del manejo de información mediante el uso de nuevas tecnologías de la información tiene o ha tenido alguna incidencia en el ejercicio de las actividades económicas, sociales o ambientales de América Latina y el Caribe.

Según datos de Cepal, las estimaciones que vinculan al producto interno bruto (PIB) con el grado de digitalización de los países, entre los años 2005 y 2013, demuestran que el impacto económico en América Latina y el Caribe ha contribuido al 4,3% del crecimiento acumulado del PIB, lo que equivale a 195.000 millones de dólares.[1894]

Dicha actividad, además, ha significado al aumento de empleos, el cual se estima ha contribuido a la creación de 900.000 puestos de trabajo anualmente en la región. Estas cifras están destinadas a crecer conforme se refuerce el ecosistema digital mundial con implementación de nuevas tecnologías y políticas que las respalden y promuevan.

Entre 2008 y 2012 el comercio a escala mundial de datos se incrementó en el 49%, mientras que las importaciones y exportaciones de bienes o servicios solo aumentaron en el 2,4%. Se ha notado que la toma de decisiones basada en datos brinda resultados más productivos en 5 a 6%.[1895]

Estudios en Europa estiman que aproximadamente 100.000 nuevos trabajos relacionados con manejo de datos serán creados al 2020. Asimismo, la adopción de *big data* en las empresas top 100 EU de manufactura podría representar un ahorro aproximado de 425 billones de euros, lo que representaría un incremento de PIB de 206 billones de euros.[1896]

El mercado global de *hardware*, *software* y servicios profesionales ligados con la implementación de *big data* alcanzará 43,7 billones euros para 2019.[1897]

Mediante la promoción de tecnologías innovadoras como el *big data* o el internet de las cosas la recopilación de datos puede llegar a ser muy valiosa para el sector privado, especialmente

[1894] CEPAL, *Ciencia, tecnología e innovación en la economía digital* (Chile, 2016).
[1895] European Commission, *Enter the data economy* (Belgium, 2017).
[1896] Ibíd.
[1897] Ibíd.

cuando la asociación de estos brinda información de interés comercial o incluso gubernamental. Dicha información puede servir para optimizar la prestación de servicios y la toma de decisiones institucionales;[1898] dicho presupuesto establece además la necesidad de implementar mecanismos de protección al uso de la información disponible a través de los medios digitales con el objeto de proteger los datos de carácter personal que puedan transitar por estos.

Los datos estadísticos previamente referidos determinan con claridad la incidencia del tránsito de datos en la economía de los países de Latinoamérica y el Caribe, así como su vertiginoso crecimiento en la región. Dicho presupuesto permite determinar que el alcance propuesto en el artículo 213 de la Constitución viabiliza la incorporación de un ente de control, vigilancia y supervisión que posibilite una efectiva protección del derecho a la protección de datos dentro del tránsito de información mediante el uso de las nuevas tecnologías de la información.

Las funciones de inspección, vigilancia y control son modalidades de ejercicio del poder de policía puesto que por medio de ellas se imponen limitaciones, que deben ser legalmente establecidas, a la actividad de los particulares con el fin de proteger el orden público y el bien común.

Las funciones de inspección, control y vigilancia son formas de intervención estatal que suelen ir acompañadas de una potestad sancionatoria, motivo por el cual la norma que asigne tales funciones debe tener rango legal.

El Estado solo puede limitar derechos en razón del reconocimiento de otros derechos, trátese de derechos individuales, sociales o colectivos. Más allá del título de habilitación del poder de ordenación o regulación estatal, este poder debe estar previsto en el marco constitucional o legal de modo claro y específico. De manera que en un Estado de derecho no existen títulos de habilitación sin más. El poder de regulación debe nacer del propio texto constitucional o legal; además, precisar cuál es el ámbito material y el alcance de esos poderes.

Los caracteres más sobresalientes del poder de policía en el Estado actual son el principio de reserva legal, la razonabilidad, la proporcionalidad, la no alteración (respetar el núcleo propio de los derechos), y el criterio pro libertad.

El control público tiene como finalidad asegurar la observancia del obrar público a reglas y principios del derecho, a los cuales debe ajustarse el poder. En la función de control es esencial la existencia de una situación de crisis para hacer uso de esta facultad, que se puede manifestar mediante la imposición de multas, sanciones o correctivos. La finalidad del control es mantener y recuperar aquellas personas que, aunque presentan una situación de crisis, tienen posibilidades reales de recuperación, o en caso de carencia de posibilidades de recuperación, busca que la disolución y liquidación se haga adecuadamente, evitando el descalabro del sector y que su desaparición no genere consecuencias desfavorables a la sociedad; en caso de generarlas, que estas se minimicen.

La Función Administrativa de Inspección es la potestad administrativa destinada a garantizar la adecuación permanente de las actividades sujetas a control a lo dispuesto por la ley, y a las

[1898] SAS, *The Value of Big Data and the Internet of Things to the UK Economy* (United Kingdom, 2016).

que se hubiera establecido en el correspondiente título habilitante, precisando que dicha garantía podrá comprender, también, las acciones necesarias para el restablecimiento de la legalidad quebrantada. Esta definición deberá complementarse, necesariamente, con una referencia al fundamento mismo de la existente o reconocimiento de su finalidad institucional que, como resulta lógico dentro de un Estado democrático de derecho, que no es otro sino la necesaria protección de un interés general fundado en la protección de los derechos fundamentales o de otros bienes constitucionalmente consagrados.

> La actividad inspectora, como toda actividad esencialmente imperativa o de autoridad, está sometida al clásico principio de legalidad administrativa, en virtud del cual es exigible la adecuada cobertura legal, es decir, la atribución por Ley a la Administración de la potestad de inspección sobre una materia, sector o ámbito determinado, precisando su alcance, extensión y los fines que ha de tutelar, y, ello sin perjuicio de reconocer, desde luego, la conveniencia de un ulterior desarrollo reglamentario de determinados aspectos de la actuación inspectora.[1899]

Por tanto, esa facultad comporta la posibilidad de solicitar información de las personas objeto de supervisión, así como de practicar visitas a sus instalaciones y realizar auditorías y seguimiento de su actividad. La vigilancia, por su parte, está referida a funciones de advertencia, prevención y orientación encaminadas a que los actos del ente vigilado se ajusten a la normativa que lo rige; finalmente, el control permite ordenar correctivos sobre las actividades irregulares y las situaciones críticas de orden jurídico, contable, económico o administrativo.

Como tales funciones, particularmente, la de control, van acompañadas de una potestad sancionatoria que les asegura eficacia. Entonces, entran en juego también otras garantías constitucionales relacionadas al debido proceso y el principio de legalidad sancionatoria.

En cualquier modelo de Estado, la función inspectora es un elemento fundamental, porque donde existe un poder que ordena y ejecuta se ha de supervisar el cumplimiento de lo ordenado, pues la vigilancia es el presupuesto de su acción real; esto constituye la esencia del poder Ejecutivo y es una tarea constante, común a todos los tipos de Estado y de Administración.[1900]

La inspección es una potestad administrativa restrictiva o limitativa de derechos. Debido a su finalidad institucional, la inspección trae consigo, siempre, aunque en diversos grados, la restricción o limitación de derechos del administrativo, el cual deberá soportarlos en la medida de su proporcionalidad. También porque su finalidad institucional pretende, es preciso siempre reiterarlo, la satisfacción de un especial y concreto interés público. Al configurarse como una atribución administrativa que traerá consigo la restricción de los derechos del ciudadano, se desprende la necesidad que su configuración se haga respetando escrupulosamente el principio de legalidad, para proteger y precautelar adecuadamente la defensa de los derechos del administrado.

Si el ejercicio de la potestad inspectora conlleva también la restricción de derechos fundamentales, deberá tenerse en cuenta, además, la necesidad de respetar el principio de

[1899] S. FERNÁNDEZ RAMOS, *La Actividad Administrativa de Inspección: el régimen jurídico general de la función inspectora* (Granada: Comares, 2002), 124.
[1900] R. RIVERO ORTEGA, *El Estado vigilante: consideraciones jurídicas sobre la función inspectora de la administración* (Madrid: Editorial Tecnos, 2000), 25-26.

reserva de ley, que obliga a que tales atribuciones sean fijadas en una norma con rango de ley.

Entre las atribuciones concedidas a la administración pública dentro del ejercicio de su función de inspección está la de adoptar medidas correctivas, como aquellas orientadas a reconducir la actividad de los administrados hacia los parámetros legalmente establecidos; es decir, a restablecer la vigencia del ordenamiento jurídico que ha sido quebrantado, siendo por dicho motivo, sustancialmente diferentes a las sanciones administrativas y, también, a las llamadas medidas cautelares.

Mientras en la sanción administrativa es, según la clásica definición de Eduardo García de Enterría y Tomás-Ramón Fernández "un mal infligido por la Administración a un administrado como consecuencia de una conducta ilegal. Este mal consistirá siempre en la privación de un bien o de un derecho imposición de una obligación de pago de un multa".[1901] Entretanto, las medidas correctivas han sido definidas como "aquellos actos de gravamen y autónomos que sujetos al principio de legalidad el ordenamiento jurídico autoriza expresamente dictar a algunas entidades ante la comisión de algún ilícito, para, independientemente de la sanción que corresponda, reestablecer al estado anterior de las cosas o reparar la legalidad afectada mediante la cancelación o reversión de los efectos externos producidos".[1902]

El artículo 132 de la Constitución de la República del Ecuador establece como atribución de la Asamblea Nacional la de aprobar como leyes las normas generales de interés común, entre otros casos, para regular el ejercicio de los derechos y garantías constitucionales.

El artículo 76, numeral 3 de la norma *ibídem*, determina que nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no este tipificado en la ley como infracción penal, administrativa o de otra naturaleza; ni se aplicará una sanción no prevista por la Constitución o la ley.

Por otra parte, el artículo 134 de la Constitución de la República del Ecuador determina en el numeral 6:

> La Asamblea Nacional aprobará como leyes las normas generales de interés común. Las atribuciones de la Asamblea Nacional que no requieren de la expedición de una ley se ejercerán a través de acuerdos o resoluciones. Se requerirá de ley en los siguientes casos: [] 6. Otorgar a los organismos públicos de control y regulación la facultad de expedir normas de carácter general en las materias propias de su competencia, sin que puedan alterar o innovar las disposiciones legales.

Entonces, con base en el principio de reserva de ley, el procedimiento de creación de la Superintendencia debe realizarse mediante un acto normativo emitido por la Asamblea Nacional del Ecuador en función de las atribuciones establecidas en los artículos 76, numeral 3), 132 y 134, numeral 6 de la Constitución de la República del Ecuador. Se observarán los presupuestos establecidos en el artículo 5 del Código Orgánico Administrativo en el cual se determina que para la creación de un órgano o una entidad administrativa se cumplirán los siguientes requisitos:

[1901] E. GARCÍA DE ENTERRÍA y T. FERNÁNDEZ, *Curso de Derecho Administrativo*, vol. II, 161.

[1902] J. MORÓN URBINA, "Los actos medida (medidas correctivas, provisionales y de seguridad) y la potestad sancionadora de la Administración". *Revista de Derecho Administrativo*, 9 (2011):157.

1. Determinación de su forma de integración y su dependencia o adscripción.

2. Delimitación de sus competencias.

3. Especificación de sus competencias.

4. Presentación de informes de los órganos competentes en materia de planificación y finanzas, cuando se requiera.

En este sentido, para el Ecuador, dada su estructura normativa y administrativa, es necesaria la creación de una Superintendencia de Protección de Datos Personales, bajo los siguientes parámetros:

CONTROL, VIGILANCIA Y SANCIÓN

Art.- Autoridad de aplicación. Créase la Superintendencia de Protección de Datos Personales, parte de la Función de Transparencia y Control Social, como un organismo técnico de control, con capacidad sancionatoria, de administración desconcentrada, con personalidad jurídica, patrimonio propio y autonomía administrativa, presupuestaria y organizativa, con jurisdicción nacional y coactiva; la que contará con amplias atribuciones para hacer cumplir la normativa de protección de datos personales y leyes conexas. La Superintendencia podrá actuar de oficio o a petición de parte.

Su domicilio será la ciudad de Quito, sin perjuicio de las oficinas que pueda establecer para su gestión desconcentrada, de conformidad con lo dispuesto en el ordenamiento jurídico vigente. No obstante lo dispuesto en este artículo, no podrán desconcentrarse las competencias normativas.

La Superintendencia, el superintendente no admitirán ninguna forma de instrucción, en el desempeño de sus funciones y en el ejercicio de sus potestades sancionatorias, correctivas o normativas.

Art.- Patrimonio.- El patrimonio de la Superintendencia se integra por:

1. Las asignaciones que constarán en el Presupuesto General del Estado;

2. Todos los bienes muebles e inmuebles que adquiera a cualquier título;

3. Los legados o donaciones que perciba de personas naturales o jurídicas; y,

4. Otros ingresos procedentes de su autogestión.

Art.- Superintendente de protección de datos personales.- El Superintendente será designado por el Consejo de Participación Ciudadana y Control Social, de la terna enviada por el Presidente de la República. Durará cinco años en sus funciones, y podrá ser reelegido por una sola vez. Será de nacionalidad ecuatoriana, acreditar título

universitario de abogado, experiencia en actividades de administración, control, o asesoría, o en el ámbito relacionado con la protección de datos personales, y encontrarse libre de inhabilidades para ejercer cargo público.

El Superintendente será la máxima autoridad administrativa, resolutiva y sancionadora de la Superintendencia de Protección de Datos Personales y ostentará su representación legal, judicial y extrajudicial de la Superintendencia.

El Superintendente presentará anualmente a la Asamblea Nacional una memoria que contenga el detalle de las principales labores realizadas por la institución y un resumen de la situación de las personas bajo su control, relacionados con el ejercicio del año anterior, de acuerdo con el reglamento.

Art.- Atribuciones del Superintendente.- El Superintendente de protección de datos personales ejercerá las siguientes atribuciones.

1. Representar judicial y extrajudicialmente a la Superintendencia.

2. Dictar las normas de control, generales y técnicas.

3. Imponer sanciones.

4. Celebrar a nombre de la Superintendencia los contratos y convenios que requiera la gestión institucional.

5. Dirigir, coordinar y supervisar la gestión administrativa de la Superintendencia.

6. Nombrar al personal necesario para el desempeño de las funciones de la Superintendencia.

7. Delegar algunas de sus facultades, siempre en forma concreta y precisa, a los funcionarios que juzgue del caso.

8. Resolver los recursos de orden administrativo.

9. Las demás establecidas en la ley y en su reglamento.

Art.- Causas para el cese de funciones del Superintendente.- El Superintendente cesará de su cargo por una de las siguientes causales: 1. Sentencia condenatoria ejecutoriada. 2. Incompatibilidad superveniente. 3. Incapacidad mental o física, debidamente comprobada por la Asamblea Nacional, que impidiere el ejercicio del cargo durante más de ciento ochenta días calendario. 4. Por censura y destitución previo enjuiciamiento político conforme la Constitución de la República. 5. Por muerte. 6. Por renuncia voluntaria.

Pese a lo expuesto, al ser, la Dirección Nacional de Registro de Datos Público, dependiente del Ejecutivo, resulta imposible que bajo un régimen de austeridad y políticas de reducción del tamaño del Estado, se propongan normativas que promuevan la creación de nuevas entidades, bajo este presupuesto el texto normativo propuesto, prevé lo siguiente:

AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES

Artículo 83.- Autoridad de Protección de Datos Personales.- La Autoridad de Protección de Datos Personales será una entidad de derecho público dependiente de la Función Ejecutiva con personería jurídica y gozará de autonomía administrativa y financiera. Su máxima autoridad será designada mediante Concurso Público de Méritos y oposición por un período fijo de 6 años y deberá cumplir con los siguientes requisitos mínimos:

a) Ser ecuatoriano o ecuatoriana de nacimiento;

b) Tener título de Abogado; y,

c) Tener título de cuarto nivel en ramas afines a la protección de datos personales.

Artículo 84.- Funciones, atribuciones y facultades.- Corresponden a la Autoridad de Protección de Datos Personales las siguientes funciones, atribuciones y facultades:

a) Ejercer la supervisión, control y evaluación de las actividades efectuadas por el responsable y encargado del tratamiento de datos personales y de las entidades certificadoras, de conformidad a lo establecido en la presente Ley, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales;

b) Conocer sobre los proyectos de normas de carácter general o técnico que se desarrollen en materia de protección de datos personales;

c) Emitir normativa general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y garantizar el ejercicio del derecho a la protección de datos personales;

d) Promover o proponer proyectos de ley o reformas en materia de protección de datos personales;

e) Autorizar y revocar la autorización de funcionamiento de entidades certificadoras, conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente;

f) Revisar, aprobar, rechazar, revocar y exigir la modificación de códigos de protección, mecanismos de certificación o sellos de confianza de datos personales, conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente;

g) Revocar las certificaciones o sellos de protección en materia de datos personales, conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente;

h) Promover una coordinación adecuada y eficaz con entidades de certificación o agentes privados encargados de la rendición de cuentas, y participar en iniciativas internacionales y regionales para la protección de la protección de los datos personales;

i) Dictar las cláusulas estándar de protección de datos, así como verificar el contenido de las cláusulas o garantías adicionales o específicas;

j) Conocer, sustanciar y resolver los reclamos interpuestos por el titular o aquellos iniciados de oficio; así como aplicar las sanciones correspondientes;

k) Atender consultas en materia de protección de datos personales;

l) Promover e incentivar el ejercicio del derecho a la protección de datos personales;

m) Ejercer el control y emitir las resoluciones de autorización para la transferencia internacional de datos;

n) Coordinar con otros organismos del sector público y privado los esfuerzos para formular y aplicar planes y políticas destinados a fortalecer la protección de datos personales;

o) Ejercer la representación internacional en materia de protección de datos personales;

p) Coordinar, promover y ejecutar programas de cooperación con organismos internacionales análogos en materia de protección de datos personales, así como con unidades nacionales relacionadas, dentro del marco de sus competencias; y ejecutar acciones conjuntas a través de convenios de cooperación nacional o internacional;

q) Prestar asistencia en asuntos relacionados con la protección de datos personales a petición de un organismo nacional o internacional, de una entidad pública o privada;

r) Emitir directrices para el diseño y contenido de la política de tratamiento de datos personales;

s) Establecer directrices para el análisis, evaluación y selección de medidas de seguridad de los datos personales;

t) Llevar un registro estadístico sobre vulneraciones a la seguridad de datos personales e identificar posibles medidas de seguridad para cada una de ellas;

u) Solicitar información sobre su gestión a responsables, encargados y entidades de certificación para el cumplimiento de sus funciones de control y demás atribuciones establecidas en la presente ley;

v) Realizar o delegar auditorías técnicas al tratamiento de datos personales de conformidad a lo establecido en la presente Ley, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales;

w) Solicitar y recabar información para el análisis y elaboración de estudios en materia de protección de datos personales;

x) Publicar periódicamente una guía de la normativa relativa a la protección de datos personales;

y) Ejercer la potestad sancionadora respecto de responsables, encargados, terceros y entidades de certificación, conforme a lo establecido en la presente ley;

z) Crear, dirigir y administrar el Registro Nacional de Protección de Datos Personales; así como, coordinar las acciones necesarias con entidades del sector público y privado para su efectivo funcionamiento;

aa) Promover la concientización en las personas y la compresión de los riesgos, normas, garantías y derechos en relación con el tratamiento y uso de sus datos personales, con especial énfasis en actividades dirigidas a grupos de atención prioritaria, tales como niñas, niños y adolescentes;

bb) Compartir con organismos internacionales análogos en materia de protección de datos personales, así como con entidades nacionales e internacionales de control o fiscalización de índole administrativa o judicial: (i) informes, (ii) información; o (iii) datos personales relacionados a procesos de investigación, en el marco de sus competencias y de conformidad con la normativa aplicable, sin que dicha transferencia constituya una vulneración al principio de confidencialidad al constituir parte de la cadena de custodia, con la finalidad exclusiva de realizar el análisis, investigación y toma de acciones legales, judiciales y las demás que fueren pertinentes, pudiendo ser además utilizada como instrumento probatorio; y,

cc) Las demás atribuciones señaladas en la Constitución y ley.

Sin embargo, en la intervención tanto del Ministro de Telecomunicaciones, Andrés Michelena como de la Mgs. Lorena Naranjo Godoy como Directora Nacional de Registro de Datos Públicos en la Comisión de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral de la Asamblea Nacional de la República del Ecuador, el día 13 de noviembre de 2019, se instó a este órgano para que propongan la generación de una autoridad que no dependa del ejecutivo. Ya que, la Asamblea Nacional al ser una Función del Estado diferente de la del Ejecutivo, no se encuentra limitada por el decreto de austeridad. En consecuencia, pueden solicitar un estudio de impacto económico de la creación de una nueva institucionalidad y evaluar que la garantía del derecho a la protección de datos personales amerita la creación de un nuevo ente y por ende la asignación de recursos.

2.10 Régimen sancionador: Infracciones administrativas, regulación y sanciones

Las Naciones Unidas, en sus recomendaciones para la regulación de los archivos de datos personales informatizados, sugieren que cada país designe “una autoridad responsable de

supervisar la observancia de los principios establecidos. Esta autoridad ofrecerá garantías de imparcialidad, independencia frente a las personas o agencias responsables de procesar y establecer los datos, y competencia técnica. En caso de violación de lo dispuesto en la ley nacional que lleve a la práctica los principios anteriormente mencionados, deben contemplarse condenas penales u otras sanciones, junto con los recursos individuales adecuados".[1903]

Estos criterios básicos son fundamentales para garantizar la vigencia de la protección de los datos personales y establecer un equilibrio con el libre flujo informacional. Es menester ahora dedicar atención al régimen sancionador como mecanismo disuasivo de la conducta que permita cumplir con los objetivos de esta normativa.

La sanción tiene una vinculación exclusiva y directa con la infracción administrativa, constituye entonces una retribución negativa identificada como tal por el ordenamiento jurídico como consecuencia de una conducta. Por tanto, cualquier situación desfavorable para el administrado que no derive de una conducta calificada como infracción administrativa por el ordenamiento jurídico no constituye una sanción de dicha naturaleza jurídica.

La infracción administrativa constituye una expresión del ejercicio de la potestad sancionadora de la cual se encuentra investido el Estado, y constituye una reacción del orden constituido al incumplimiento al deber de contribución que todo ciudadano tiene frente a la sociedad en función del bien jurídico que se busca proteger.

El ejercicio de la facultad sancionadora del Estado tiene una finalidad esencialmente represiva o de castigo; por tanto, constituye un acto desfavorable que afecta la esfera jurídica de una particular con una finalidad represora frente a una infracción o conducta ilícita.

Goldschmidt ha conceptualizado al derecho penal administrativo como "el conjunto de aquellos preceptos por medio de los cuales la Administración del Estado a la que se ha confiado la promoción del bien público o del Estado, enlaza, dentro del marco de la autorización jurídico estatal, en forma de preceptos jurídicos, una pena como consecuencia administrativa a la contravención de un precepto administrativo como tipo".[1904]

Es importante señalar que una de las principales características de la pena administrativa es que su aplicación o castigo no corresponde a la autoridad judicial, sino a la administrativa, siendo la administración la que debe aplicarlas.

En este marco es preciso establecer si las garantías contempladas en el derecho penal, como máxima expresión del ejercicio del *ius puniendi*, son aplicables al régimen sancionatorio administrativo. Así, se han manejado diversas posiciones doctrinales en torno a la identificación de los elementos comunes entre la infracción administrativa y la penal; al respecto Andrés Ascárate ha señalado:

> Se observa la intención de definir a la infracción administrativa en su comparación con el delito; lo cual presupone que se concibe, apriorísticamente, de una observación de ambos fenómenos, que delito e infracción no son idénticos pero sí similares. En consecuencia, se procura dotar de contenido al concepto de infracción administrativa,

[1903] Asamblea General de Naciones Unidas, http://200.33.14.21:83/20121122060127-12869.pdf, 95.
[1904] Citado en H. MATTES, *Problemas de Derecho Penal Administrativo. Bases Fundamentales*, t. I (Santiago de Chile: Editorial Jurídica de Chile, 1996), 191.

> a través de una comparación con el delito penal que permita observar similitudes o diferencias. Algunos autores ven diferencias en elementos como la finalidad de la sanción o el bien jurídico protegido (GOLDSCHMIDT, BIELSA O NÚÑEZ), y designan esta deferencia como "ontológica". Mientras que otros consideran que no existe esa distinción, que también suele denominar "cualitativa" y explican discrepancias subjetivas (MARIENHOFF, DIEZ), en el tipo de sanción (COMANDIRA, ROXIN, SOLER, GRECCO), en la gravedad de la protección o de la pena (ZAFFARONI, GARCÍA DE ENTERRÍA).
>
> Tanto los que asimilan a la infracción y al delito como sus detractores reconocen la necesidad de incorporar al análisis la distribución de competencia entre la Nación y las Provincias propia de nuestro país.[1905]

En ese orden de ideas, Juan Carlos Cassagne, siguiendo la posición de Goldschmidt, ha señalado que "Existe una distinción cualitativa entre los delitos judiciales e infracciones administrativas, determina por la naturaleza de las cosas sobre la base de que, mientras en los primeros el contenido material del injusto se encuentre en el daño (o en la situación de peligro), concreto y mesurable, inferido de un bien jurídico, en las infracciones se está ante la violación del deber de obediencia o de colaboración por parte de los particulares con la administración pública".[1906]

Así, el *ius puniendi*, en sentido subjetivo, no es otra cosa que la facultad que en el sistema jurídico se reconoce para sentar y aplicar castigos; en cambio, en sentido objetivo, se trata del conjunto de las normas sancionadoras así establecidas y de las prácticas de su aplicación con arreglo a las normas del sistema jurídico y aplicación de los principios que rigen el ejercicio de la facultad sancionatoria del Estado con la finalidad de garantizar el efectivo ejercicio de los derechos reconocidos a los administrados.[1907]

En Ecuador estas diversas posiciones doctrinarias han encontrado un cauce formal de aplicación con base en los siguientes presupuestos:

El artículo 424 de la Constitución de la República del Ecuador determina que "La Constitución y los tratados internacionales de derechos humanos ratificados por el Estado que reconozcan derechos más favorables a los contenidos en la Constitución, prevalecerán sobre cualquier otra norma jurídica o actos del poder público".

Por otra parte, con fecha 12 de agosto de 1977, Ecuador ratificó el Pacto de San José de Costa Rica, cuyo ámbito de aplicación material quedó definido, entre otros fallos, en el dictado por la Corte Interamericana de Derechos Humanos dentro del caso Baena Ricardo vs Panamá en el cual se demandó la supuesta violación, por parte del Estado panameño, de los artículos 8. (Garantías Judiciales), 9. (Principio de Legalidad y de Retroactividad), 10. (Derecho a Indemnización), 15. (Derecho de Reunión), 16. (Libertad de Asociación) y 25. (Protección Judicial), en cuyos párrafos 106 y 127 la Corte señaló:

[1905] Cuestiones Preliminares para el Estudio de la Infracción Administrativa, accedido 9 de octubre de 2018, http://www.derecho.uba.ar/docentes/pdf/estudios-de-derecho/0011-edp-azcarate.pdf

[1906] J. CASSAGNE, *Derecho Administrativo*, t. II (Lima: Ed. Palestra), 561.

[1907] Sobre el uis puniendi: su fundamento, sus manifestaciones y sus límites, accedido 9 de octubre de 2018, https://revistasonline.inap.es/index.php?journal=DA&page=article&op=view&path%5B%5D=9600&path%5B%5D=9601

106. En relación con lo anterior, conviene analizar si el artículo 9o. de la Convención es aplicable a la materia sancionatoria administrativa, además de serlo, evidentemente, a la penal. Los términos utilizados en dicho precepto parecen referirse exclusivamente a esta última. Sin embargo, es preciso tomar en cuenta que las sanciones administrativas son, como las penales, una expresión del poder punitivo del Estado y que tienen, en ocasiones, naturaleza similar de éstas. Unas y otras implican menoscabo, privación o alteración de los derechos de las personas, como consecuencia de una conducta ilícita. Por lo tanto, en un sistema democrático es preciso extremar las precauciones para que dichas medidas se adopten con estricto respeto a los derechos básicos de las personas y previa una cuidadosa verificación de la efectiva existencia de la conducta ilícita. Asimismo, en aras de la seguridad jurídica es indispensable que la norma punitiva, sea penal o administrativa, exista y resulte conocida, o pueda serlo, ante de que ocurran la acción y omisión que la convienen y que se pretende sancionar. La calificación de un hecho como ilícito y la fijación de sus efectos jurídicos deben ser preexistentes a la conducta del sujeto al que se considera infractor. La calificación de un hecho como ilícito y la fijación de sus efectos jurídicos deben ser preexistentes a la conducta del sujeto al que se considera infractor. De lo contrario, los particulares no podrían orientar su comportamiento conforme a un orden jurídico vigente y cierto, en el que se expresan el reproche social y las consecuencias de éste. Éstos son los fundamentos de los principios de legalidad y de irretroactividad desfavorable de una norma punitiva.[1908]

[...] 127. Es un derecho humano el obtener todas las garantías que permitan alcanzar decisiones justas, no estando la administración excluida de cumplir con este deber. Las garantías mínimas deben respetarse en el procedimiento administrativo y en cualquier otro procedimiento cuya decisión pueda afectar los derechos de las personas".

Bajo los antecedentes expuestos y siendo que los fallos emitidos por la Corte Interamericana en relación con la interpretación de las disposiciones constantes en la Convención Interamericana de Derechos Humanos son vinculantes, y con base en lo dispuesto en el artículo 424 de la Constitución de la República, se puede concluir que las garantías inherentes al derecho penal son plenamente aplicables en el marco del ejercicio de la potestad sancionatoria administrativa. En este sentido, es necesario referirse a los principios que rigen el ejercicio de la potestad sancionadora por parte del Estado:

a) *Legalidad*.- Con relación a este principio el artículo 226 de la Constitución de la República del Ecuador establece que las instituciones del Estado, sus organismos, dependencias, las servidoras y servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Entretanto, el artículo 29 del Código Orgánico Administrativo recoge el Principio de Tipicidad, el cual determina que son infracciones administrativas las acciones y omisiones previstas en la ley; dicho cuerpo normativo determina la aplicación del principio de reserva de ley, en función del cual corresponde de forma exclusiva y excluyente al legislador establecer las acciones u omisiones que pueden ser calificadas como infracciones administrativas, así como determinar la consecuencia jurídica que dicha inobservancia pueda derivar para el administrado.

[1908] Corte IDH, Baena Ricardo, párr. 106, accedido 9 de octubre de 2018, www.corteidh.or.cr/docs/resumen/baena_ricardo.pdf

b) *Debido procedimiento.*- El artículo 76 de la Constitución de la República del Ecuador establece las garantías del debido proceso dentro de su margen de aplicación tanto a los procesos jurisdiccionales como administrativos; dichas disposiciones son aplicables a todo proceso en el que se determinen derechos y obligaciones de cualquier orden.

c) *Razonabilidad.*- A través de la aplicación de este principio se busca establecer si una actuación estatal es o no jurídicamente la más adecuada para perseguir un determinado fin. Se trata de determinar si es constitucionalmente admisible la intervención estatal o cuál es el grado de intervención compatible con el respeto a los derechos.

d) *Irretroactividad.*- Ha sido identificado como un principio sustantivo del derecho administrativo sancionador, mediante el cual se garantiza a las personas la posibilidad de conocer las normas y las consecuencias jurídicas de sus actos. Este principio encuentra su fundamento en la aplicación del derecho a la seguridad jurídica, contemplado en el artículo 82 de la Constitución de la República del Ecuador el cual en su tenor literal dispone: "Art. 82.- El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por la autoridades competentes." En el mismo sentido, en el artículo 76, numeral 6) de la Constitución reconoce como garantía básica del debido proceso que "3. Nadie podrá ser juzgado ni sancionado por un acto y omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal, administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la ley. Sólo se podrá juzgar a una persona ante y juez o autoridad competente y con observancia del trámite propio de cada procedimiento." Conforme se desprende de la normativa previamente referida, la Constitución de la República del Ecuador estableció el marco jurídico mediante el cual reconoció implícitamente la aplicación del principio de irretroactividad sobre la base de la aplicación del derecho a la seguridad jurídica que asiste a los ciudadanos de contar con normas previas, claras, públicas y aplicadas por autoridades competentes, así como el ejercicio de las garantías del debido proceso. Dicha garantías incluyen la imposibilidad de aplicar sanciones de índole administrativa que deriven de un acto u omisión, que no se encuentre tipificado como infracción administrativa, cuyo alcance se extiende además a la aplicación de sanciones que no se encuentren previstas en la Constitución ni en la ley.

e) *Presunción de licitud.*- Es una presunción de hecho, en función de la cual se supone que la persona a quien se le imputa el cometimiento de una infracción administrativa conserva su cualidad de inocencia hasta que se demuestre su culpabilidad. Este principio guarda relación con el principio de impulso de oficio del procedimiento administrativo que determina, entre otros parámetros, el deber de llegar a establecer la verdad material y revierte la carga de la prueba en favor del administrado.

f) *No bis in ídem.*- Guarda relación con la prohibición de que un mismo hecho resulte sancionado más de una vez; es decir, que se imponga una duplicidad de sanciones en los casos en los que se desprende identidad subjetiva y objetiva. El Código Orgánico Administrativo ha recogido los principios de debido proceso, legalidad, tipicidad, irretroactividad, proporcionalidad y razonabilidad, los cuales deben ser aplicados dentro de los procedimientos administrativos sancionatorios que sean llevados a cabo por las entidades que ejerzan funciones material y formalmente administrativas.

De otro lado, la normativa latinoamericana de aquellos países en los cuales se regulan el derecho a la protección de datos personales[1909] desarrollan tres tipos de responsabilidad: civil, administrativa y penal. Para lo cual se establecen infracciones debidamente tipificadas con

[1909] Argentina, Colombia, Costa rica, Ecuador, Guatemala, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay.

sus respectivas sanciones por el incumplimiento de las obligaciones relativas a la protección de los datos personales. Estas conductas transgresoras en su mayoría se sancionan con multas de contenido económico.

Solo Ecuador y Guatemala, países que regulan la protección de datos personales pero que no tienen ley específica, carecen de sanciones administrativas.

En el caso de Ecuador, mediante la garantía constitucional del *habeas data*, por el daño causado, se puede atribuir responsabilidad y su correspondiente reparación integral; asimismo, se puede asignar responsabilidad penal por medio del tipo penal de revelación ilegal de bases de datos.[1910]

El RGPD, al igual que la normativa latinoamericana, establece tres tipos de responsabilidad: administrativa, civil y penal. La forma de garantizar estas dos últimas se instaura mediante el principio de responsabilidad y en el mecanismo de tutela judicial efectiva, por el cual los interesados pueden presentar acciones en vía civil o penal de ser procedentes.

Acerca de la responsabilidad administrativa, el citado RGPD establece varios criterios orientadores para que la autoridad de control imponga sanciones administrativas como las de: atender las circunstancias de cada caso individual; la naturaleza, gravedad y duración de la infracción; la naturaleza, alcance o propósito de la operación de tratamiento de que se trate; las categorías de los datos de carácter personal afectados por la infracción; el número de interesados afectados; el nivel de los daños y perjuicios que hayan sufrido los interesados afectados; el dolo, la intencionalidad o negligencia en la infracción; el grado de responsabilidad, del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado aplicando los principios de privacidad por defecto y por diseño y de seguridad. Asimismo, la reincidencia, el incumplimiento de medidas previas; cualquier otro factor agravante aplicable a las circunstancias del caso, como los perjuicios financieros o las directas o indirectas, a través de la infracción; cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados; el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción. También la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida; la adhesión a códigos de conducta o a mecanismos de certificación aprobados; cualquier otro factor atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, mediante la infracción.

El régimen sancionatorio administrativo del RGPD establece que la autoridad de control puede, de forma simultánea o independiente, imponer las siguientes sanciones administrativas:

a) multas administrativas;

b) poderes correctivos como: advertencias, apercibimientos, órdenes de operaciones de tratamiento, de prohibición o limitación temporal o definitiva del tratamiento, de atender las solicitudes de ejercicio de los derechos del interesado, de comunicar al interesado las

[1910] Artículo 229, Código Orgánico Integral Penal del Ecuador.

violaciones de la seguridad de los datos personales, órdenes de rectificar o suprimir datos personales o limitar su tratamiento, notificar las medidas a quienes se hayan comunicado datos personales; retirar directamente u ordenar que no se emita o que se retiren, de ser el caso, una certificación si no se cumplen o dejan de cumplirse los requisitos; y, ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

Respecto de las multas administrativas, mediante un análisis de ponderación el RGPD ha establecido que determinadas infracciones ameritan una cuantía más elevada de multa respecto de otras. Entonces, se establece las siguientes condiciones aplicables de manera general:

d) Un monto máximo de multa que oscila entre 10.000.000 EUR o para empresa una cuantía equivalente al 2% del volumen de negocio total anual global del ejercicio financiero anterior, como máximo, para aquellas infracciones cometidas por responsables o encargados de tratamiento que hubieran incumplido las obligaciones propias del tratamiento, del delegado de Protección de Datos, de las certificaciones, o de los códigos de conducta.

e) Un monto máximo de multa que oscila entre 20.000.000 EUR o para empresas una cuantía equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior, como máximo, para aquellas infracciones cometidas por responsables o encargados de tratamiento que hubieran incumplido lo atinente a los principios del tratamiento, derechos de los interesados, transferencias de datos personales a un destinatario en un tercer país o una organización internacional, disposiciones relativas a situaciones específicas de tratamiento, incumplimiento de poderes correctivos, o de poderes de investigación o de resoluciones sobre sanciones dictadas con poderes correctivos.

De lo analizado, se rescata la categorización sencilla en infracciones leves y graves, además el mecanismo de cálculo de la cuantía de la multa para que sirva de modelo para la versión ecuatoriana de normativa.

Debe rescatarse también la iniciativa de adaptación del derecho español[1911] por el cual se determina que están sujetos al régimen sancionador: los responsables de los tratamientos; los encargados de los tratamientos; los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea, las entidades de certificación, las entidades acreditadas de supervisión de los códigos de conducta; no será de aplicación al delegado de protección de datos el régimen sancionador.

Adicionalmente, se establece que los artículos relativos a principios, derechos y obligaciones constituyen infracciones que prescribirán a los tres años. Se interrumpirá la prescripción con el conocimiento del interesado de un procedimiento sancionador iniciado.

Luego de lo analizado, se propone el siguiente texto normativo:

MEDIDAS CORRECTIVAS, INFRACCIONES Y RÉGIMEN SANCIONATORIO

[1911] N.º 70751, el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

Artículo 72.- Objeto y ámbito de aplicación.- Los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, están sujetos a medidas correctivas, infracciones y al régimen sancionatorio establecido en el presente Capítulo.

En el caso de entidades pertenecientes al sector público, las resoluciones que determinen medidas correctivas o aplicación de régimen sancionatorio, deberán ser comunicada a la máxima autoridad de la institución responsable del tratamiento de datos personales con la finalidad de que se inicien los procedimientos disciplinarios en contra de los servidores o funcionarios, por cuya acción u omisión se hubiese incurrido en alguna de las infracciones establecidas en la presente Ley, sin perjuicio de la responsabilidad civil, administrativa y/o penal a la que hubiere lugar.

Artículo 73.- Medidas correctivas.- En caso de incumplimiento de las obligaciones previstas en la presente Ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia; o, transgresión a los derechos y principios que componen al derecho a la protección de datos personales, la Autoridad de Protección de Datos Personales dictará medidas correctivas con el objeto de reestablecer el derecho vulnerado y evitar que la conducta se produzca nuevamente, sin perjuicio de la aplicación de las correspondientes sanciones administrativas.

Las medidas correctivas podrán consistir, entre otras, en:

El cese del tratamiento bajo determinadas condiciones o plazos; y,
La imposición de medidas técnicas, jurídicas, organizativas o administrativas tendientes a garantizar un tratamiento adecuado de datos personales.

Artículo 74.- Implementación.- La Autoridad de Protección de Datos Personales, en el marco de esta Ley, implementará para cada caso las medidas correctivas, previo informe de la unidad técnica competente, que permita corregir, revertir o eliminar las conductas contrarias a la presente Ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

Para la aplicación de las medidas correctivas se seguirán las siguientes reglas:

Para el caso de infracciones leves se aplicará a los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, únicamente medidas correctivas; en el caso de incumplimiento de dichas medidas correctivas o que éstas fueren cumplidas de forma tardía, parcial o defectuosa, la Autoridad de Protección de Datos Personales, aplicará la sanción establecida en el artículo 79 de la presente Ley;

En el caso de que los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, se encuentren incursos en el presunto cometimiento de una infracción leve y éstos consten dentro del Registro Único de Responsables y Encargados Incumplidos; la Autoridad de Protección de Datos Personales activará directamente el procedimiento administrativo sancionatorio haciendo constar dentro

de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida; y,

En el caso de que los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, se encuentren incursos en el presunto cometimiento de una infracción grave, la Autoridad de Protección de Datos Personales activará directamente el procedimiento administrativo sancionatorio haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida.

Sección 1a
Del responsable

Artículo 75.- Infracciones leves.- Se consideran infracciones leves las siguientes:

No tramitar, tramitar fuera del plazo previsto o negar injustificadamente las peticiones o quejas realizadas por el titular;

No notificar a la Autoridad de Protección de Datos Personales y al titular las vulneraciones de seguridad y protección de datos personales cuando no exista afectación a los derechos fundamentales y libertades individuales de los titulares;

No mantener disponible políticas de protección de datos personales afines al tratamiento de datos personales;

No mantener actualizado el Registro Nacional de Protección de Datos Personales de conformidad a lo dispuesto en la presente Ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia; y,

Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales.

Artículo 76.- Infracciones graves.- Se consideran infracciones graves las siguientes:

No implementar requisitos, mecanismos o herramientas administrativas, técnicas, físicas, organizativas y jurídicas a fin de garantizar que el tratamiento de datos personales se realice conforme la presente Ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;

Utilizar información o datos para fines distintos a los declarados;

No cumplir lo dispuesto en códigos de protección, mecanismos de certificación, sellos de protección, cláusulas estándar de protección de datos, cláusulas o garantías adicionales o específicas y normas vinculantes;

Proceder a la comunicación de datos personales, sin cumplir con los requisitos y procedimientos establecidos en la presente Ley, su reglamento, directrices,

lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;

No utilizar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales, las particularidades del tratamiento y de las partes involucradas;

No realizar evaluaciones de impacto al tratamiento de datos;

No implementar medidas técnicas, organizativas o de cualquier índole necesaria para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones a la seguridad de los datos personales que hayan sido identificadas;

No notificar a la Autoridad de Protección de Datos Personales y al titular las vulneraciones a la seguridad y protección de datos personales cuando afecte los derechos fundamentales y libertades individuales de los titulares;

No implementar protección de datos desde el diseño y por defecto;

No suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;

Elegir al encargado del tratamiento de datos personales que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales;

No consignar en el Registro Nacional de Protección de Datos Personales lo dispuesto en la presente Ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;

No designar al Delegado de Protección de Datos Personales;

No permitir o no contribuir a la realización de auditorías o inspecciones, por parte del auditor acreditado por la Autoridad de Protección de Datos Personales;

El incumplimiento de las medidas correctivas o el cumplimiento de éstas de forma tardía, parcial o defectuosa; siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por infracción leve.

Sección 2a
Del encargado

Artículo 77.- Infracciones leves.- Se consideran infracciones leves las siguientes:

No asistir al responsable para que éste cumpla con su obligación de atender solicitudes que tengan por objeto el ejercicio de los derechos del titular frente al tratamiento de sus datos personales;

No facilitar el acceso al responsable del tratamiento de datos personales a toda la información referente al cumplimiento de las obligaciones establecidas en la presente

Ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;

No permitir o no contribuir a la realización de auditorías o inspecciones, por parte del responsable del tratamiento de datos personales o de otro auditor autorizado por éste o por la Autoridad de Protección de Datos Personales; y,

Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales.

Artículo 78.- Infracciones graves.- Se consideran infracciones graves las siguientes:

No tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente Ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;

No tratar datos personales de conformidad con lo previsto en el contrato que mantenga con el responsable del tratamiento de datos personales, inclusive en lo que respecta a la transferencia o comunicación internacional;

No suscribir contratos de confidencialidad y manejo adecuado de datos personales con el personal a cargo del tratamiento de datos personales, o quién tenga conocimiento de los datos personales;

No implementar mecanismos destinados a mantener la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;

No implementar medidas preventivas y correctivas en la seguridad de los datos personales a efecto de evitar vulneraciones;

No suprimir los datos personales transferidos o comunicados al responsable del tratamiento de los datos personales una vez haya culminado su encargo;

No cumplir lo dispuesto en códigos de protección, mecanismos de certificación, sellos de protección, cláusulas estándar de protección de datos, cláusulas o garantías adicionales o específicas y normas vinculantes; y,

Proceder a la comunicación de datos personales, sin cumplir con los requisitos y procedimientos establecidos en la presente Ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

El incumplimiento de las medidas correctivas o el cumplimiento de éstas de forma tardía, parcial o defectuosa; siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por infracción leve.

Artículo 79.- Sanciones por infracciones leves.- La Autoridad de Protección de Datos Personales impondrá las siguientes sanciones administrativas en el caso de

verificarse el cometimiento de una infracción leve conforme a los presupuestos establecidos en el presente Capítulo:

Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones detalladas en el artículo 75 y 77 de la presente Ley Orgánica serán sancionados con una multa de 1 a 10 salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente.

Si el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero, es una entidad de Derecho Privado o una Empresa Pública se aplicará una multa de entre el 3% y el 9% calculada sobre su volumen de negocio, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad para lo cual deberá verificar los siguientes presupuestos:

La intencionalidad, misma que se establecerá en función a la conducta del infractor;

Reiteración de la infracción; es decir, cuando el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero; hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar;

La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,

Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

Artículo 80.- Sanciones por infracciones graves.- La Autoridad de Protección de Datos Personales impondrá las siguientes sanciones administrativas en el caso de verificarse el cometimiento de una infracción grave conforme a los presupuestos establecidos en el presente Capítulo:

Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones detalladas en el artículo 76 y 78 de la presente Ley Orgánica serán sancionado con una multa de entre 10 a 20 salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente.

Si el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero, es una entidad de Derecho Privado o una Empresa Pública se aplicará una multa de entre el 10% y el 17% calculada sobre su volumen de negocio, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la multa

aplicable en función del principio de proporcionalidad para lo cual deberá verificar los siguientes presupuestos:

La intencionalidad, misma que se establecerá en función a la conducta del infractor; Reiteración de la infracción; es decir, cuando el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero; hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar;

La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,

Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

En el caso de que el responsable, encargado del tratamiento de datos personales o un tercero de ser el caso; sea una organización sin domicilio ni representación jurídica en el territorio ecuatoriano, la Autoridad de Protección de Datos Personales notificará de la Resolución con la cual se establezca la infracción cometida a la autoridad de protección de datos, o quien hiciera sus veces, del lugar en donde dicha organización tiene su domicilio principal, a fin de que sea dicho organismo quien sustancie las acciones y/o procedimientos destinados al cumplimiento de las medidas correctivas y sanciones a las que hubiere lugar.

Artículo 81.- Volumen de Negocio.- A efectos del Régimen Sancionatorio de la presente Ley, se entiende por volumen de negocio, a la cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del impuesto sobre el valor agregado y de otros impuestos directamente relacionados con la operación económica.

Artículo 82.- Medidas provisionales o cautelares.- La Autoridad de Protección de Datos Personales podrá aplicar medidas provisionales de protección o medidas cautelares contempladas en la norma procedimental administrativa.

2.11 Transferencia internacional de datos

Se entiende como transferencia internacional de datos al intercambio de datos entre países. México, Perú y Uruguay incluyen en su normativa una definición. Además, México determina la necesidad de formalizar la transferencia mediante la suscripción de cualquier instrumento jurídico que cumpla la normativa y que avale el intercambio.

Por su parte, las Naciones Unidas sugieren que las salvaguardas para proteger la intimidad entre dos países deben ser similares para garantizar el flujo informacional, sin mayor limitación que las medidas relacionadas con la protección de dicha intimidad". [1912] Si bien, la

[1912] Asamblea General de Naciones Unidas, http://200.33.14.21:83/20121122060127-12869.pdf.

referencia no es al derecho de protección de datos, la reciprocidad se instituye como principio aplicable al flujo transfronterizo entre países.

La OEA reconoce la responsabilidad en el flujo transfronterizo de datos cuando determina que los Estados miembros cooperarán entre sí en la creación de mecanismos y procedimientos que aseguren que los controladores de datos que operen en más de una jurisdicción puedan ser efectivamente hechos responsables por el cumplimiento de estos principios.[1913]

Por su parte, el RGPD adiciona otros actores, pues la necesidad del intercambio transfronterizo de datos personales se produce no solo entre la Unión Europea y Estados miembros con terceros países, sino también con organismos internacionales.

Esta norma también determina que este intercambio de información es fundamental para la expansión del comercio y la cooperación internacionales; que es un mecanismo de universalización del sistema de protección de los datos de carácter personal; que pretende evitar los riesgos de un tratamiento transfronterizo que se produce casi de forma natural, en especial respecto de transferencias ulteriores, para lo cual reconoce el principio general de las transferencias como criterio básico que organiza y orienta este sistema.

Para facilitar la aplicación eficaz de la legislación sobre protección de datos personales, las garantías adecuadas y los derechos y libertades fundamentales, y mejorar la relación entre terceros países, organizaciones internacionales se tomarán medidas apropiadas como las de crear mecanismos de cooperación internacional; prestarse mutuamente asistencia a escala internacional, en particular mediante la notificación de reclamaciones; la remisión de reclamaciones; la asistencia en las investigaciones, y el intercambio de información.

Para tal efecto, el régimen de transferencia internacional se basa en la declaración de países que cumplen con niveles adecuados de protección desde la perspectiva del estándar europeo como el de más alto nivel o el cumplimiento de ciertas condiciones necesarias para garantizar una adecuada transferencia.[1914] En este mismo sentido, Argentina, Colombia, México, Perú, República Dominicana y Uruguay establecen como condición necesaria que permite el intercambio internacional de datos que el país receptor proteja los datos conforme la normativa del país emisor, o que cumpla un estándar para que sea posible la transferencia.

Para eso, se establecen mecanismos de transferencia:

a) *Transferencias basadas en una decisión adecuada*. Es un mecanismo de transferencia fronteriza de datos, por el cual la Comisión, como máximo organismo encargado de velar la vigencia y aplicación de los reglamentos emitidos por la Unión Europea, verifica y califica si un tercer país, territorio, uno o varios sectores específicos de ese tercer país, o la organización internacional tiene un nivel adecuado de protección de los datos personales, mediante una decisión de adecuación recogida en un acto de ejecución. Para tal efecto, realizará una evaluación de nivel adecuado, que consiste en identificar elementos ineludibles, que no pueden omitirse, estos son: a) Respeto a las libertades individuales y a los derechos fundamentales; b) Autoridades de control independiente; y c) Vigencia de normativa internacional como tratados, convenios, pactos, instrumentos de cooperación, u otras

[1913] Asamblea General OEA, 86 Período Ordinario de Sesiones, CJI/doc. 474/15 rev.2 Río de Janeiro, Brasil, 26 marzo 2015, *Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales*, http://www.oas.org/es/sla/ddi/docs/cji-doc_474-15_rev2.pdf.
[1914] BOE, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*, 27 de abril de 2016.

obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes. La declaración de país con nivel adecuado, también la instituyen países como Colombia y Uruguay, en los cuales los órganos de control son los encargados de realizar la evaluación del nivel adecuado de protección de un tercer país, para verificar que este ofrezca garantías suficientes respecto a la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como sobre el ejercicio de los respectivos derechos, o la consignación y el respeto de los principios rectores de la ley citada; además como medidas técnicas de seguridad y confidencialidad, tal como señala Perú.

b) *Transferencias mediante garantías adecuadas*. Es un mecanismo de transferencia transfronteriza de datos que opera cuando no existe una decisión de adecuación recogida en un acto de ejecución dictado por la Comisión, por el cual, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país, mediante garantías adecuadas para el interesado como: a) La observancia de requisitos de protección de datos, adecuados al tratamiento dentro de la Unión; b) El respeto por los derechos de los interesados, adecuados al tratamiento dentro de la Unión; c) Derechos exigibles y acciones legales efectivas a disponibilidad de los interesados; d) El derecho a obtener una reparación administrativa o judicial efectiva; e) El derecho a reclamar una indemnización en la Unión o en un tercer país; f) El cumplimiento de los principios generales relativos al tratamiento de los datos personales; g) El cumplimiento de los principios de protección de datos desde el diseño y por defecto. Para la consecución de este mecanismo, se requiere de un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos, normas corporativas vinculantes, cláusulas tipo de protección de datos, cláusulas o garantías adicionales, códigos de conducta aprobados o mecanismos de certificación.

c) *Normas corporativas vinculantes*. Una figura propia de los grupos empresariales o de la unión de empresas de actividad económica conjunta es el de normas corporativas vinculantes que les permita un trabajo coordinado, armónico, coherente entre las distintas organizaciones que las conforman respetando los principios esenciales y derechos aplicables que otorguen garantías adecuadas para las transferencias. Es un mecanismo de transferencia transfronteriza de datos, dictado por la autoridad de control. La autoridad de control competente aprobará normas corporativas vinculantes cuyo contenido mínimo contemple: datos de contacto; las transferencias o conjuntos de transferencias de datos; categorías de datos personales; tipo de tratamientos y fines; tipo de interesados afectados; nombre del tercer o los terceros países. Asimismo, la aplicación de los principios generales en materia de protección de datos, los derechos de los interesados y los medios para ejercerlos; cláusula de responsabilidad; la existencia de normas corporativas y su carácter jurídicamente vinculante; mecanismos de supervisión; verificación del cumplimiento de las normas vinculantes; mecanismos de comunicación a la autoridad de control. También, mecanismos de cooperación con la autoridad de control; mecanismos para informar a la autoridad de control de cualquier requisito jurídico de aplicación, que probablemente tenga un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, formato, procedimientos para el intercambio de información, entre otros.

d) *Excepciones para situaciones específicas*. Si bien la regla general es que no se podrá autorizar transferencias o comunicaciones de datos personales a terceros países por parte de responsables o encargados regidos por el RGPD, incluso si esta transferencia se solicita mediante sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país. Únicamente será reconocida o ejecutable en cualquier modo la citada sentencia o la decisión de autoridad administrativa de un país, si existe un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro.

Sin embargo, se señalan varias situaciones específicas que, pese a que no existe una decisión de adecuación aprobada por la Comisión, tampoco garantías adecuadas presentadas por el

responsable o el encargado o una autoridad de control, ni aún normas corporativas vinculantes se puede realizar una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente si se cumple alguna de las condiciones siguientes que se va a analizar: a) Consentimiento explícito del interesado, como ocurre también con la normativa colombiana, de República Dominicana, México, Nicaragua, Perú y Uruguay; b) Celebración y ejecución de un contrato entre interesado y responsable de tratamiento, en el mismo sentido también Colombia, República Dominicana, México, Nicaragua, Perú y Uruguay; c) Ejecución de medidas precontractuales entre interesado y responsable de tratamiento; d) Interés público, como también señalan Colombia, México, Nicaragua Perú, República Dominicana y Uruguay, incluido el tema tributario como señala República Dominicana; e) Ejercicio de reclamaciones; f) Para proteger los intereses vitales del interesado o de otras personas cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; g) Los registros públicos; h) Mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular, como señala México y Nicaragua; i) Se realice entre responsables para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales por parte de entidades públicas, conforme señalan México, Nicaragua y Uruguay; j) Asuntos judiciales, para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial o ante autoridad competente, así como la procuración o administración de justicia, conforme señala Colombia, México, Nicaragua y República Dominicana; k) Colaboración judicial internacional, reconocido por Argentina, República Dominicana, Nicaragua, Perú y Uruguay; l) Datos de salud, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios: Argentina, Colombia, República Dominicana, Nicaragua, Perú y Uruguay. Perú, además, condiciona que los datos deben ser disociados; m) Transferencias bancarias y bursátiles: conforme consta en Argentina, Colombia, República Dominicana, Nicaragua, Perú y Uruguay; n) Prevención, investigación y persecución del crimen organizado, terrorismo y narcotráfico, administración de los bienes incautados, decomisados y abandonados, delitos contra la seguridad del Estado, vado de activos, corrupción, trata de personas y demás delitos, por lo que se autoriza el intercambio de datos cuando la transferencia sea legalmente exigida para la investigación y persecución de estos delitos, conforme señala Argentina, República Dominicana, México, Nicaragua, Perú y Uruguay.

e) Transferencias sin el amparo a los que no les ampara ningún mecanismo transfronterizo de datos a terceros países. Para la transferencia de datos a terceros países a los que no les ampara ni una decisión de adecuación aprobada, ni garantías adecuadas, ni corporativas vinculantes, ni aun los casos de excepción específica, solo deben ser posibles en "casos aislados, cuando ninguno de los otros motivos para la transferencia sean aplicables". Únicamente podrá llevarse a cabo esta transferencia que no tiene ningún tipo de amparo, a riesgo del responsable de tratamiento: a) si no es repetitiva; b) afecta solo a un número limitado de interesados; c) es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento, siempre y cuando no prevalezcan los intereses o derechos y libertades del interesado; no será aplicable por autoridades públicas, puesto que es indispensable que exista un ley como base jurídica para el tratamiento de datos personales por parte de las autoridades públicas.

Sobre consideraciones adicionales de protección: México establece la necesidad de que la transferencia de datos se realice implementando avisos de privacidad, por lo cual se solicita autorización y debe informarse sobre las finalidades para las cuales se obtienen sus datos.

Asimismo, México señala que entre responsable y encargado no se requerirá informar al titular, ni contar con su consentimiento para la cesión entre ellos.

Finalmente, Costa Rica, Ecuador, Guatemala, Panamá no señalan norma alguna relativa al flujo transfronterizo de datos.

Luego del análisis realizado se propone una normativa, para la cual se invoca el Estándar Iberoamericano de Protección de Datos Personales bajo la premisa de que cada Estado debe establecer expresamente límites o autorizaciones a las transferencias internacionales de categorías de datos personales por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros; así como por cuestiones de interés público[1915] o, como se vio en el análisis, antes de otros criterios de atribución.

> **Artículo 60.- Transferencia o comunicación internacional de datos personales.-** La transferencia o comunicación internacional de datos personales será posible si se sujeta a lo previsto en el presente capítulo, la presente Ley o la normativa especializada en la materia, propendiendo siempre al efectivo ejercicio del derecho a la protección de datos personales.
> **Artículo 61.- Criterios para declarar el nivel adecuado de protección.-** Para declarar de nivel adecuado de protección a países u organizaciones, la Autoridad de Protección de Datos Personales emitirá resolución motivada, en la cual se verificará la existencia de los siguientes presupuestos:
>
> Que cuente con normativa que promueva y garantice el ejercicio de derechos fundamentales y libertades individuales;
>
> Que cuente con una autoridad estatal independiente que garantice y promueva la efectiva tutela del derecho a la protección de datos personales;
>
> Que cuente con normativa especializada en materia de protección de datos personales;
>
> Que sea parte de Acuerdos o instrumentos internacionales vinculantes ratificados por un tercer país u organización que generen obligaciones respecto al tratamiento y trasferencia o comunicación de datos personales, siempre que estos establezcan un estándar igual o mayor de protección en favor del titular, más allá de su origen o nacionalidad; y,
>
> Que posea legislación específica en materia seguridad nacional y defensa del Estado, que establezca mecanismos de control y verificación del acceso de las autoridades públicas a los datos personales de sus ciudadanos.
>
> La resolución de nivel adecuado de protección deberá contemplar mecanismos de revisión periódica, al menos cada cinco años, para garantizar el derecho a la protección de datos personales. También establecerá acciones conjuntas entre las autoridades de ambos países con el objeto de prevenir, corregir o mitigar el tratamiento indebido de datos en ambos países.

[1915] Red Iberoamericana de Protección de Datos Personales, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.

Artículo 62.- Transferencia o comunicación internacional de datos personales a países declarados como nivel adecuado de protección.- Por principio general se podrán transferir o comunicar datos personales a países u organizaciones que brinden niveles adecuados de protección, conforme a los criterios establecidos en el artículo precedente.

Artículo 63.- Transferencia o comunicación mediante garantías adecuadas.- Este mecanismo de transferencia o comunicación transfronteriza de datos personales opera cuando no existe una resolución de nivel adecuado de protección, en su lugar el responsable o encargado del tratamiento de datos personales deberá tomar medidas para compensar la falta de protección de datos en un tercer país u organización mediante garantías adecuadas para el titular, debiendo cumplir al menos con las siguientes:

Observancia de principios, derechos y obligaciones en el tratamiento de datos personales siempre que estos cumplan con un estándar igual o mayor de protección;

Efectiva tutela del derecho a la protección de datos personales, a través de la disponibilidad permanente de acciones administrativas o judiciales; y,

El derecho a solicitar la reparación integral, de ser el caso.

Para la consecución de este mecanismo se requiere de instrumentos jurídicos vinculantes y exigibles entre autoridades y responsables del tratamiento de datos personales tales como: normas corporativas vinculantes, cláusulas estándar de protección de datos, cláusulas o garantías adicionales o específicas, códigos de protección, mecanismos de certificación, sellos de protección de datos personales aprobados.

Corresponde a la Autoridad de Protección de Datos Personales dictar el contenido de las cláusulas estándar de protección de datos, así como la verificación de cláusulas o garantías adicionales o específicas acordadas entre las partes.

La Autoridad de Protección de Datos Personales aprobará códigos de protección, mecanismos de certificación y sellos de protección de datos personales.

Para el cumplimiento de lo previsto en el presente artículo, se considerarán los derechos, garantías y principios de la presente Ley, como requisitos y condiciones mínimas para la transferencia o comunicación internacional.

Artículo 64.- Normas corporativas vinculantes.- Los responsables o encargados del tratamiento de datos personales podrán presentar a la Autoridad de Protección de Datos Personales normas corporativas vinculantes, específicas y aplicadas al ámbito de su actividad, en las cuales, para su aprobación, deberán cumplir las siguientes condiciones:

Ser de obligatorio cumplimiento para el responsable de tratamiento, la totalidad del grupo empresarial al que ésta pertenezca, sus empresas asociadas y cualquier otra empresa a la que eventualmente transfieran datos personales;

Brindar a los titulares los mecanismos adecuados para el ejercicio de sus derechos relacionados al tratamiento de sus datos personales, observando las disposiciones constantes en la presente Ley;

Incluir una enunciación detallada de las empresas filiales que, además del responsable del tratamiento, pertenecen al mismo grupo empresarial. Además se incluirá la estructura y los datos de contacto del grupo empresarial o joint venture dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

Incluir el detalle de las empresas encargadas del tratamiento de datos personales, las categorías de datos personales a ser utilizados, así como el tipo de tratamiento a realizarse y su finalidad;

Enunciar de forma expresa el carácter jurídicamente vinculante de tales normas a nivel nacional e internacional;

Observar en su contenido todas las disposiciones de la presente ley referentes a principios de tratamiento de datos personales, medidas de seguridad de datos, requisitos respecto a transferencia o comunicación internacional y transferencia o comunicación ulterior a organismos no sujetos a normas corporativas vinculantes;

Contener la aceptación por parte del responsable o del encargado del tratamiento de los datos personales o de cualquier miembro de su grupo empresarial sobre su responsabilidad por cualquier violación de las normas corporativas vinculantes. El responsable o encargado del tratamiento de datos personales no será responsable si éste demuestra que el acto que originó los daños y perjuicios no le es imputable.

Incluir los mecanismos en que se facilita al titular la información clara y completa, respecto a las normas corporativas vinculantes y sus efectos jurídicos;

Incluir las funciones de todo delegado de protección de datos designado o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o del joint venture dedicadas a una actividad económica conjunta bajo un mismo control, así como los mecanismos y procesos de supervisión y tramitación de reclamaciones;

Detallar los procesos o procedimientos en vía administrativa o judicial que le asistan;

Enunciar de forma detallada los mecanismos establecidos en el grupo empresarial o empresas afiliadas que permitan al titular verificar efectivamente el cumplimiento de las normas corporativas vinculantes. Entre estos mecanismos se incluirá auditorías continuas de protección de datos y aquellos métodos técnicos que brinden acciones correctivas para proteger los derechos del titular. Los resultados de las auditorías serán de acceso público, debidamente publicados y se pondrán a disposición de la Autoridad de Protección de Datos Personales en la periodicidad establecida en el Reglamento a la presente Ley;

Incluir los mecanismos para cooperar de forma coordinada con la Autoridad de Protección de Datos Personales y el responsable del tratamiento de los datos personales; y,

Incluir la declaración y compromiso del responsable del tratamiento de los datos personales de promover la protección de datos personales entre sus empleados con formación continua.

La Autoridad de Protección de Datos Personales definirá el formato y los procedimientos para la transferencia o comunicación de datos realizada por parte de los responsables, los encargados y las autoridades de control en lo relativo a la aplicación de las normas corporativas vinculantes a las que se refiere este artículo.

Cualquier cambio a ser realizado a estas normas deberá ser previamente aprobado por la Autoridad de Protección de Datos Personales y notificado al titular conforme a los mecanismos señalados por el responsable de tratamiento en su solicitud de aprobación.

Artículo 65.- Casos excepcionales de transferencias o comunicaciones internacionales.- En aquellos casos donde no se apliquen los artículos 54 y 55 de la presente Ley, la Autoridad de Protección de Datos Personales podrá autorizar transferencias o comunicaciones internacionales de datos personales, en los siguientes casos:

A países u organismos internacionales que brinden garantías adecuadas para la protección de datos personales sin que necesariamente exista una ley específica o Autoridad de Protección de Datos Personales, para lo cual será necesaria la suscripción de un convenio o tratado internacional;

Cuando los datos personales sean requeridos para el cumplimiento de competencias institucionales con finalidad pública;

Cuando el titular haya otorgado su consentimiento explícito a la transferencia o comunicación propuesta, tras haber sido informado de las finalidades del tratamiento y posibles riesgos para él de dichas transferencias o comunicaciones internacionales, debido a la ausencia de una resolución de nivel adecuado de protección y de garantías adecuadas;

Cuando la transferencia internacional tenga como finalidad el cumplimiento de una obligación legal o regulatoria;

Cuando la transferencia internacional de datos personales sea necesaria para la ejecución de una obligación contractual entre el titular y el responsable del tratamiento de datos personales, o para la ejecución de medidas de carácter precontractual adoptadas a solicitud del titular;

Cuando la transferencia internacional de datos personales sea necesaria para la celebración o ejecución de un contrato, en interés del titular entre el responsable del tratamiento de datos personales y otra persona natural o jurídica;

Cuando la transferencia sea necesaria por razones de interés público;

Cuando la transferencia internacional sea necesaria para la colaboración judicial internacional;

Cuando la transferencia internacional sea necesaria para la cooperación dentro de la investigación de infracciones;

Cuando la transferencia internacional es necesaria para el cumplimiento de compromisos adquiridos en procesos de cooperación internacional entre Estados;

Transferencias bancarias y bursátiles;

Cuando la transferencia internacional de datos personales sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones, acciones administrativas o jurisdiccionales y recursos; y,

Cuando la transferencia internacional de datos personales sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 66.- Control continuo.- La Autoridad de Protección de Datos Personales en acciones conjuntas con la academia, realizará reportes continuos sobre la realidad internacional en materia de protección de datos personales. Dichos estudios servirán como elemento de control continuo del nivel adecuado de protección de datos personales de los países u organizaciones que ostenten tal reconocimiento.

En caso de detectarse que un país u organización ya no cumple con un nivel adecuado de protección conforme los principios, derechos y obligaciones desarrollados en la presente ley, la Autoridad de Protección de Datos Personales procederá a emitir la correspondiente resolución de no adecuación, a partir de la cual no procederán transferencias de datos personales, salvo que operen otros mecanismos de transferencia conforme lo dispuesto en el presente capítulo.

La Autoridad de Protección de Datos Personales publicará en cualquier medio, de forma permanente y debidamente actualizado, una lista de países, organizaciones, empresas o grupos económicos que garanticen niveles adecuados de protección de datos personales.

3. Conclusión

Pese a la existencia de una norma constitucional que reconoce el derecho a la protección de datos personales[1916] y de la garantía constitucional del *habeas data*,[1917] es evidente que la falta de normativa legal, de jurisprudencia e incluso de normativa sectorial mantiene en

[1916] Ecuador, *Constitución de la República del Ecuador*, 2008, artículo 66.
[1917] Ibíd, artículo 92.

estado de abandono a los datos personales de los ecuatorianos. Esta afirmación es grave puesto que los datos personales son parte misma de un individuo, manifestación de su libertad informativa, de su libre desarrollo de la personalidad, y facultan otros derechos fundamentales y libertades individuales; por tanto, esta situación de laguna normativa nos retrasa, no solo desde la perspectiva de los emprendimientos, la innovación, la competitividad del país, sino desde protección y salvaguarda de derechos de los titulares y de la construcción de una cultura de protección que permita que la sociedad camine hacia un régimen que garantice el libre flujo de información con respeto a la persona.

Entonces, Ecuador carece de un marco de protección frente al avance de las TIC en la cotidianeidad de los ecuatorianos, lo que torna indispensable la construcción de una cultura de protección de datos personales, que desarrolle derechos, principios y obligaciones.

En consecuencia, es evidente que el Estado debe dictar una normativa que establezca un sistema que responda a las condiciones particulares de este derecho, esto es el de ser un derecho complejo, porque no tiene un núcleo unívoco, pues está constituido por varios derechos e incluso garantías que lo integran, que además siguen en evolución y se complementan en la medida en la que la sociedad se desarrolla. Uno de los núcleos primigenios de este derecho, aunque no el único, es la autodeterminación informativa. Las personas pueden decidir qué datos entregan y con qué finalidad, siempre que hayan sido debidamente informadas, y que medie su consentimiento para que estos sean tratados y utilizados. De existir un abuso la persona puede retirar el consentimiento, o si ya no tercia la voluntad del titular de los datos, esta persona puede simplemente retirar, cancelar, actualizar u oponerse a la recogida o tratamiento de sus datos personales. En todos estos casos se visualizan lo que en legislaciones de corriente europea se reconoce como derechos ARCO (actualización, rectificación, cancelación u oposición), y que en otros lugares, especialmente en Latinoamérica, se ha reconocido mediante la acción de *habeas data*, que tutela estos derechos a nivel jurisdiccional por medio de una garantía constitucional.

Conforme este investigación las limitaciones establecidas en la ley resultan ser un mecanismo muy útil para determinar cuál es el contenido mínimo del derecho; en este caso, del derecho a la protección de datos personales.

Una las finalidades de determinar el contenido esencial es la de identificar los casos de excepción que ameritan una versión acotada del derecho sin que sea posible eliminar elementos considerados esenciales, pero si otros que si bien ayudan a su desarrollo su omisión no significa un irrespeto al derecho en sí mismo. Este es el caso de lo dispuesto en el artículo 23 del RGPD, denominado Limitaciones, por el cual el derecho de la Unión o de los Estados miembros, incluida en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, aplicable a los responsables o el encargado del tratamiento, podrá limitar mediante medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 del RGPD (acceso, rectificación, supresión, derecho al olvido, oposición, portabilidad, limitación al tratamiento, no soportar decisiones individuales automatizadas, incluida la elaboración de perfiles). Así como, las contenidas en el artículo 34 relativas a las notificaciones de las violaciones de seguridad y las del artículo 5 respecto a los principios en su relación con los citados derechos y obligaciones, incluso en aquellas conexas.

Un sistema de protección que, mediante mecanismos de identificación de riesgo, produzca su minimización debido a la implementación de mecanismos preventivos. Además de ocurrir

transgresiones o daños se minimicen sus consecuencias, y se evada su masiva difusión en una sociedad hiperconectada.

Toda vez que los mecanismos de control y de sanción no tienen como finalidad únicamente la de recuperar recursos a título de multa, sino que su verdadera intención es la de constituirse como elementos disuasivos de la voluntad, que eviten futuras transgresiones. Asimismo, un sistema de control y vigilancia del cumplimiento de las obligaciones de los responsables contribuye a establecer un sistema de mejora continua que potencie los mecanismos de resguardo y el espíritu preventivo que permita anticipar consecuencias negativas, al mismo tiempo que facilita un uso adecuado y productivo de las innovaciones tecnológicas.

Igualmente, el derecho a la protección de datos personales se puede violentar por acción u omisión, y en consecuencia, es también una obligación del Estado procurar que no se produzcan daños debido a la incorrecta actuación de responsables o encargados de bases de datos sean estos entes públicos o privados, para lo cual será preciso establecer una institucionalidad y regularización interna que determine un uso adecuado de los datos personales en todas las fases del ciclo del dato; es decir, en la recogida, tratamiento, almacenamiento, seguridad, cesión, entre otras.

Asimismo, los Estados tienen la obligación de establecer o mantener mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado.[1918] Esta obligación se refiere no solo a la creación de una institucionalidad propia, independiente y especializada que pueda realizar actividades de control y vigilancia para el cumplimiento de la normativa que regula un manejo adecuado de los datos personales, sino que también hace alusión a normas, leyes, reglas, procedimientos, prácticas que con este enfoque de transparencia se materialicen para la efectiva vigencia de los derechos; además, a la utilización de tecnologías, métodos o sistemas que deben implementarse desde el diseño y por defecto para proteger los datos personales y, al mismo tiempo, garantizar su tráfico en bienestar de la sociedad.

En consecuencia, es necesario un sistema de protección de datos avanzado, que garantice la prevención del daño mediante contenido que clarifique los deberes y responsabilidades de los responsables y encargados de las bases de datos; que empodere a sus titulares con la finalidad de construir en conjunto una sociedad respetuosa de los datos personales y de los derechos individuales de sus titulares. Así como, permita por medio del flujo informacional el desarrollo social, cultural, económico, tecnológico, la innovación y la competitividad.

[1918] Asamblea General de las Naciones Unidas, "Resolución A/C.3/68/L.45/Rev.1 sobre el Derecho a la Privacidad en la Era Digital".

CONCLUSIONES

1. El primer antecedente del derecho a la protección de datos personales es la privacidad, un derecho orientado a resarcir daños producidos a personas que se han visto afectadas ante la intromisión de terceros en su esfera personal o íntima; posteriormente, con el reconocimiento de la intimidad como derecho en la Carta Fundamental de Derechos Humanos, se evidenció la necesidad de ampliar el ámbito de protección para los individuo; es así que históricamente, ante las transgresiones palpables respecto al manejo de información fue imperante reconocer a la autodeterminación informativa como un derecho autónomo, otorgando la capacidad a las personas de decidir sobre su información, para finalmente, dar origen al derecho a la protección de datos personales, con una gama amplia de elementos que permitan salvaguardar integralmente a los seres humanos frente al tratamiento de sus datos.

2. Una evolución mundial que no ha sido ajena para el Ecuador, que si bien ha avanzado muy lentamente en la temática, ha hecho avances significativos a la hora de reconocer al derecho a la protección de datos personales como autónomo y distinto de la intimidad o privacidad, conforme lo establece la Constitución de la República del año 2008. Desde el nacimiento republicano del Estado ecuatoriano en 1830 las múltiples constituciones paulatinamente han incorporado, en su catálogo, derechos, que atienden a necesidades sociales, políticas e ideológicas, con el objetivo de proteger la dignidad de las personas. Es así como, en el ámbito de los derechos asociados a la privacidad, se reconoció a la inviolabilidad de domicilio en 1830, la inviolabilidad de la correspondencia en 1835, el derecho al honor en 1845, el derecho a la intimidad en 1967el derecho a la imagen y a la voz en 1996, así como adicionalmente, ese mismo año se incorporó al *habeas data* como garantía constitucional orientada a efectivizar los mismos.

3. De la breve descripción normativa de las Constituciones ecuatorianas y de su encuadre histórico, podemos concluir que el derecho a la inviolabilidad del domicilio es una de las primeras formas de compresión de la esfera privada de las personas; y por lo tanto, una aproximación a la protección de lo privado, con un especial enfoque respecto de las libertades políticas.

4. A pesar de que, el derecho a la protección de datos personales fue reconocido como derecho fundamental en el año 2008, el Ecuador hasta el año 2019, no ha logrado contar con normativa orientada a regular su ejercicio, por lo que ha sido necesario evaluar su contenido esencial y aplicación en la práctica; de lo que se puede destacar que la Constitución de la República refleja a la autodeterminación informativa como parte de su naturaleza, así como la necesidad de desarrollar en normas de menor jerarquía elementos que puedan encuadrar el camino correcto para su aplicabilidad.

5. Por otra parte, la Corte Constitucional, en el ejercicio de sus atribuciones, al momento de resolver aquellos casos en los que se pretende activar la garantía jurisdiccional *habeas data*, han interpretado aspectos específicos del derecho a la protección de datos personales; sin embargo, muchas de estas sentencias tienen a ser insuficientes e incompletas, esto da cuenta de la necesidad de desarrollar normativa especializada en la materia que permita el efectivo ejercicio de este derecho.

6. Con la expansión del acceso a las nuevas tecnologías de información y comunicación, los datos se han posicionado como aquella materia prima vital para este nuevo ecosistema digital, esto ha ocasionado que se planteen nuevas formas de cómo proteger todos los derechos que se generan en el flujo de estos datos; en ese sentido han ocasionado tal impacto, que los Estados se han encontrado en la obligación de readecuar sus legislaciones e incluso sus matrices productivas, con el objetivo de estar a la par del desarrollo tecnológico en el escenario internacional.

7. Es así como, los Estados han tomado básicamente dos modelos para la protección de los derechos constituidos en el flujo de datos; el modelo anglosajón-reactivo de la *privacy* y el modelo europeo-preventivo. En América Latina, a través de pronunciamientos de los informes de las Relatorías a la Libertad de Expresión, de las sentencias dictadas por la Corte Interamericana de Derechos Humanos y de las resoluciones de la Organización de Estados Americanos se colige que, aún no se reconoce, el derecho a la protección de datos personales sino que se concibe únicamente el derecho a una vida privada. Esto, debido a que los Organismos Internacionales se encuentran aún cobijados bajo instrumentos internacionales de derechos humanos que establecían normas generales de protección de derechos fundamentales, como la Convención Americana de Derechos Humanos, misma que bajo una visión del derecho a la privacidad como matriz de protección de otros derechos, han denotado una línea en sus pronunciamientos.

8. No obstante, los Estados con el avance del comercio internacional a través de las tecnologías de la información y comunicación, se han visto en la necesidad de ampliar su espectro de protección, migrando esa concepción del derecho a la privacidad como mecanismo ideal de garantía, al sistema europeo que prevé la protección de datos personales como derecho fundamental; de tal manera que ya no lo conciben como un nivel máximo e incluso exagerado de protección sino, como un nivel adecuado e incluso mínimo de protección de derechos.

9. En consecuencia, los Estados latinoamericanos han ido paso a paso adecuando sus normas desde el rango constitucional, para aterrizar en legislaciones más garantistas que permiten el adecuado flujo y tratamiento de datos, que viabilizan a su vez el establecer niveles adecuados de protección, más alineados al modelo europeo; obligando tanto a sus pares como a organismos internacionales de la región, a adecuar sus legislaciones, acuerdos y pronunciamientos al sistema preventivo de protección de derechos que apuntala al derecho a la protección de datos personales como un derecho fundamental autónomo e instrumental.

10. El derecho a la protección de los datos personales en América Latina tiene a su vez una doble modalidad de protección, esto, debido a que por su origen, la forma de garantizar este derecho en la región se ha facilitado a través del *habeas data*; que se ha plasmado en las legislaciones como derecho tanto como garantía, una doble funcionalidad que ha permitido que en su desarrollo no solo se lo determine como una acción procesal sino como un derecho instrumental que garantiza el ejercicio de otros derechos como el de acceso, rectificación, autodeterminación informativa y el derecho a la protección de datos personales.

11. Sin embargo, existen también Estados como Colombia, Argentina y México, que a través de la garantía de la tutela y el amparo han tratado de absorber el campo de

protección de la garantía del *habeas data* de manera que por intermedio de estas garantías tutelan el derecho a la protección de datos personales y aquellos derechos que devienen de este.

12. En la otra esquina se encuentran aquellos Estados que han reconocido el derecho a la protección de datos personales como un derecho fundamental dentro de sus textos constitucionales, lo que habilita un sistema más adecuado para la garantía de este derecho, pues lo deslinda totalmente de concepciones de privacidad e intimidad que en legislaciones no tan contemporáneas en América Latina se sigue conservando para hacerse efectivas a través de mecanismos procesales como el *habeas data.*

13. Por su parte, existen asimismo, Estados que han adoptado por plasmar en sus textos constitucionales y legales el derecho a la protección de datos personales como derecho fundamental; así como, el *habeas data* como derecho y garantía lo que inclusive inintencionalmente ha ocasionado que se amplíe el campo de efectiva protección para el derecho a la protección de datos de carácter persona.

14. Razón por la cual se ha dotado a los sistemas de protección de una singular integralidad, ya que ha permitido que el derecho a la protección de datos personales se traspole de la esfera de la intimidad y privacidad, hacia un ámbito autónomo, sin que se deje de lado el amplio ámbito de protección que se ha dado históricamente a estos derechos; así como la inclusión de otros derechos como el de la imagen, la voz e incluso la honra; confluyendo en un mecanismo de protección que garantice su efectivo respeto y cumplimiento.

15. En Latinoamérica aún se debaten temas superados como el contenido esencial propio del derecho a la intimidad y el derecho a la protección de datos personales. Con similar proceso evolutivo, el derecho a la protección de datos personales tiene en la intimidad sus antecedentes inmediatos; sin embargo, es mediante la definición de su contenido esencial que se ha construido un derecho diferente basado, sobre todo, en la autodeterminación informativa.

16. El derecho a la protección de datos personales en Latinoamérica no fue concebido, en principio, como un derecho fundamental autónomo, independiente, complejo e instrumental de origen jurisprudencial; sino que ha sido incorporado sobre la base de una evolución constante que ha pasado por reformas constitucionales y legales marcadas por la influencia europea; así como el desarrollo de una escasa jurisprudencia que ha intentado en cierta forma explicar el contenido mínimo de este derecho.

17. La protección de datos personales en América Latina ha tenido una línea primigenia similar a la europea debido a que sus orígenes se remontan a la intimidad, pasando por el reconocimiento de un contenido esencial distinto a este, que conllevó al nacimiento de la autodeterminación informativa como un derecho que no podía ser cobijado por la misma protección de la intimidad debido a que superaba la mera injerencia arbitraria y que encontró en el derecho a la protección de datos personales el mecanismo idóneo para su efectivo goce.

18. El desarrollo inminente de la tecnología ha causado tal rebelo en la doctrina y jurisprudencia latinoamericana que los mecanismos que comúnmente se tenían como

suficientes para proteger a la esfera del individuo en estos nuevos entornos han quedado en muchos casos inocuos, motivo por el cual la protección de datos personales se ha concebido como aquella herramienta por la cual se pueda contrarrestar el ámbito del poder informático.

19. Es así como, Latinoamérica debe lograr una paulatina armonización de las diferentes normativas que permitan una adecuada protección de los datos de carácter personal en la región, para lo cual, se debe incluir el derecho fundamental en aquellas constituciones en las que todavía no se reconoce, así como el desarrollo de su normativa específica, que prevea mecanismos de control y protección para este derecho, lo que conlleva también la creación de instancias administrativas y organismos especializados dedicados a la protección y promoción de este derecho; para que a través de ellos se establezcan políticas públicas en favor de los derechos que garantiza este derecho instrumental; así como la necesidad de que se busquen espacios, convenios, acuerdos y demás instrumentos que viabilicen la efectiva garantía del mismo.

20. Es estrictamente necesario que Latinoamérica comience a construir un frente único, armónico y eficiente, por el intermedio de organismos regionales que establezcan políticas de protección de datos y marquen una cultura de protección adecuada de las personas y un libre flujo informacional que garantice el desarrollo económico, social y cultural de la región.

21. En el caso específico de Ecuador a pesar de la existencia de un doble ámbito de garantía del derecho a la protección de datos personales, al reconocerlo como derecho fundamental y viabilizarlo a través de la garantía jurisdiccional del *habeas data* es notorio que al carecer de una normativa específica en la materia que permita el desarrollo de este derecho y el establecimiento de una autoridad que emita directrices al respecto de su efectivo cumplimiento, así como la falta de desarrollo jurisprudencial que ilumine el actuar de los responsables del tratamiento de datos, deja a la deriva el ejercicio de este derecho, permitiendo que sea confundido e incluso violentado.

22. El no contar con una legislación específica en materia de protección de datos personales no solo genera que no se esté salvaguardando los derechos de las personas; sino que afecta el desarrollo y garantía de otros derechos que son parte misma de un individuo, manifestación de su libertad informativa, de su libre desarrollo de la personalidad, y facultan otros derechos fundamentales y libertades individuales; situación que nos retrasa, no solo desde la perspectiva de los emprendimientos, la innovación, la competitividad del país, sino desde protección y salvaguarda de derechos de los titulares y de la construcción de una cultura de protección que permita que la sociedad camine hacia un régimen que garantice el libre flujo de información con respeto a la persona.

23. El Ecuador se encuentra no solo vulnerable al no poder competir en el mercado internacional frente a otros Estados que tienen normativas específicas en protección de datos personales e inclusive han obtenido certificaciones que les avalan el tener un nivel adecuado de protección; sino al potencial crecimiento de las Tecnologías de la Información y Comunicación, dejando en indefensión a las personas que desean

acudir a mecanismos adecuados de garantía de sus derechos que se encuentran establecidos en una Constitución garantista de derechos.

24. Es evidente que el Estado debe dictar una normativa que establezca un sistema que responda a las condiciones particulares del derecho a la protección de datos personales, esto es el de ser un derecho complejo, porque no tiene un núcleo unívoco, pues está constituido por varios derechos e incluso garantías que lo integran, que además siguen en evolución y se complementan en la medida en la que la sociedad se desarrolla; un derecho autónomo, pues se deslinda de la clásica visión de la privacidad e intimidad, e instrumental pues garantiza y efectiviza el ejercicio de otros derechos y garantías de las personas.

25. El Ecuador necesita una normativa que determine un sistema de protección que, mediante mecanismos de identificación de riesgo, minimice los riesgos debido a la implementación de mecanismos preventivo; así como, minimice las consecuencias de los daños o transgresiones y se evada su masiva difusión en una sociedad hiperconectada. En ese sentido es necesario un sistema que conlleve mecanismos de control y de sanción que se constituyan como elementos disuasivos de la voluntad, que eviten futuras transgresiones. Asimismo, un sistema de control y vigilancia del cumplimiento de las obligaciones que contribuya a establecer un sistema de mejora continua que potencie los mecanismos de resguardo y de reacción que permita el flujo y tratamiento adecuado de datos personales.

26. Es necesario que los Estados reconozcan la obligación de procurar que no se produzcan daños tanto por acción u omisión a los derechos de las personas, entre ellos el de la protección de datos personales, para lo cual será preciso establecer una institucionalidad y regularización interna que determine un uso adecuado de los datos personales en todas las fases del ciclo del dato; que sea propia, independiente y especializada que pueda realizar actividades de control y vigilancia, que establezca un ámbito de seguridad a sus titulares con la finalidad de construir en conjunto una sociedad respetuosa de los datos personales y de los derechos individuales de sus titulares.

27. Como resultado del análisis de la legislación comparada se pudo concluir que el modelo idóneo para lograr una ley adaptada a la realidad ecuatoriana, era el europeo, puesto que bajo el reconocimiento de la protección de datos como un derecho, resultaba inaplicable visiones de autorregulación o de incorporación de medidas únicamente cuando se ha producido el daño. Es por eso que, ha sido imperante analizar el contenido esencial del derecho a la protección de datos personales en el marco de la Unión Europea, del que colige una armonía al homologar el criterio de que la autodeterminación informativa es la piedra angular de este derecho

28. Como epílogo de esta investigación, la identificación y análisis: del contenido esencial del derecho a la protección de datos personales; de las características que definen y facilitan la implementación de cada uno de los principios y derechos que conforman este derecho complejo; de las precisiones, mejores prácticas e innovaciones generadas en aras de desarrollar un modelo de protección equilibrado han permitido obtener conclusiones que han contribuido directamente en la elaboración del Anteproyecto de Ley Orgánica de Protección de Datos Personales

para el Ecuador. En el cual, la Dirección Nacional de Registro de Datos Públicos, entidad a la cual esta autora lidera desde octubre de 2017, a través de un proceso de construcción participativa, ha integrado a todos los actores interesados, obteniendo de ellos las necesidades y visiones nacionales y los imperiosos consensos que permitan entregar una propuesta normativa que, fiel al espíritu del derecho a la protección de datos personales, recoja las condiciones y especificidades de la realidad latinoamericana y ecuatoriana sin perder el norte de construir un sistema de protección que garantice derechos a los titulares y al mismo tiempo promueva el flujo informativo. Este texto fue entregado al ente rector de las telecomunicaciones, quien a su vez, lo presentó al órgano legislativo el 19 de septiembre de 2019 y actualmente es el Proyecto de Ley Orgánica de Protección de Datos Personales para el Ecuador. Esperamos que en los siguientes meses se produzca el debate legislativo y se apruebe como Ley para el Ecuador.

Bibliografía:

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Carácter de dato personal de correo electrónico institucional. Informe 0437/2010".

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Carácter de dato personal de la dirección IP. Informe 327/2003".

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Guía de Videovigilancia", fecha de consulta 22 noviembre 2017 en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Informe Jurídico 61/2008".

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Memoria 2001", fecha de consulta 21 enero 2017, en http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2001/MEMORIA_2001.pdf.

ALESSANDRI RODRÍGUEZ, A.; SOMARRIVA UNDURRAGA, M.; VODANOVIC H., A.; ALESSANDRI RODRÍGUEZ, A., *Tratado de derecho civil: partes preliminar y general*, 6. ed., 1. ed. de Editorial Jurídica de Chile, Editorial Jurídica de Chile, Santiago, 1998.

ALMUZARA ALMAIDA, C, *Estudio práctico sobre la protección de datos de carácter personal*, 2a ed., Editorial Lex Nova, Valladolid, 2007.

ÁLVAREZ CONDE, E., *Curso de Derecho constitucional. Vol. 1, Vol. 1,* Tecnos, Madrid, 2008.

APARICIO PÉREZ, M.; BARCELÓ I SERRAMALERA, M. (eds.), *Curso de derecho constitucional*, Atelier, Barcelona, 2012.

APARICIO SALOM, J., *Estudio sobre la protección de datos*, Aranzadi, Cizur Menor, Navarra, 2013.

ASALE, R.-, "Diccionario de la lengua española - Edición del Tricentenario", *Diccionario de la lengua española*, fecha de consulta 18 enero 2017, en http://dle.rae.es/?id=LYB2BS5|LYF57Ax.

ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 50].

ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 64].

ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 67].

ASAMBLEA CONSTITUYENTE 2008 DE ECUADOR, [Acta No. 76].

ASAMBLEA NACIONAL CONSTITUYENTE 1998 DE ECUADOR, [Acta No. 47].

ASAMBLEA NACIONAL CONSTITUYENTE 1998 DE ECUADOR, [Acta No. 81].

ASAMBLEA NACIONAL CONSTITUYENTE DE 1967 DE ECUADOR, [Acta No. 46].

ASAMBLEA NACIONAL CONSTITUYENTE DE 1967 DE ECUADOR, [Acta No. 47].

ASAMBLEA NACIONAL CONSTITUYENTE DE 1977 DE ECUADOR, [Acta No. 30].

ASAMBLEA NACIONAL CONSTITUYENTE DE 1998 DE ECUADOR, [Acta No. 46].

ASAMBLEA NACIONAL CONSTITUYENTE DE 1998 DE ECUADOR, [Acta No. 80].

ASAMBLEA NACIONAL DEL ECUADOR, [Código Civil Codificado, Registro Oficial Suplemento 46 de 24-jun.-2005, Última modificación: 08 de julio de 2019], *Asamblea Nacional del Ecuador*, fecha de consulta 18 febrero 2018, en http://www.asambleanacional.gob.ec/es/leyes-aprobadas.

ASAMBLEA NACIONAL DEL ECUADOR, [Código Orgánico General de Procesos, Suplemento -- Registro Ofi cial Nº 506 -- Viernes 22 de mayo de 2015], *Asamblea Nacional del Ecuador*, fecha de consulta 18 febrero 2018, en http://www.asambleanacional.gob.ec/es/leyes-aprobadas.

ASAMBLEA NACIONAL DEL ECUADOR, [Código Orgánico Integral Penal, Suplemento, Registro Oficial Nº 180, Lunes 10 de febrero de 2014], *Asamblea Nacional del Ecuador*, fecha de consulta 18 febrero 2018, en http://www.asambleanacional.gob.ec/es/leyes-aprobadas.

ASAMBLEA NACIONAL DEL ECUADOR, [Ley de Seguridad Pública y del Estado. Ley 0, Registro Oficial Suplemento No. 35 de 28 de septiembre de 2009], *Lexis Ecuador*, fecha de consulta 22 noviembre 2017, en www.silec.com.ec.

ASAMBLEA NACIONAL DEL ECUADOR, [Ley Orgánica de Garantías y Control Constitucional, Segundo Suplemento, Registro Oficial Nº 52, jueves 22 de Octubre del 2009], *Asamblea Nacional del Ecuador*, fecha de consulta 18 febrero 2018, en http://www.asambleanacional.gob.ec/es/leyes-aprobadas.

ASAMBLEA NACIONAL ECUADOR, [Ley 0, Ley del Sistema Nacional de Registro de Datos Públicos, Registro Oficial Suplemento 162 de 31-mar.-2010, Ultima modificación: 12-sep.-2014], *Lexis Ecuador*, 2010, fecha de consulta 22 noviembre 2017, en www.silec.com.ec.

AVILA SANTAMARÍA, R.; ACOSTA, A.; MARTÍNEZ, E., *El neoconstitucionalismo transformador: el estado y el derecho en la Constitución de 2008*, Primera edición, Abya-Yala, Universidad Politécnica Salesiana : Universidad Andina Simón Bolívar, Quito, 2011.

AYALA MORA, E., *Historia, tiempo y conocimiento del pasado: estudio sobre periodización general de la historia ecuatoriana una interpretación interparadigmática.*, Corporacion Editora Nacional, Quito, 2014.

AYALA MORA, E., *Resumen de historia del Ecuador*, 1. ed, Corporación Editora Nacional, Quito, 1993.

BENAVIDES ORDÓÑEZ, J.; ESCUDERO SOLIZ, J. (eds.), *Manual de justicia constitucional ecuatoriana*, Corte Constitucional del Ecuador, Centro de estudios y difusión, Quito, 2013.

BERLIN, I., *Cuatro ensayos sobre la libertad*, Alianza, Madrid, 1998.

BORJA Y BORJA, R., *Derecho Constitucional Ecuatoriano*, vol. I, 1979.

CARRASCO DURÁN, M.; PÉREZ ROYO, J., *Curso de derecho constitucional*, Atelier, Barcelona, 2012.

CARRASCO DURÁN, M.; PÉREZ ROYO, J., *Curso de derecho constitucional*, Atelier, Barcelona, 2012.

CASARES SUBIA, MARÍA PAULINA, [La protección de datos genéticos y su impacto en los derecho humanos", fecha de consulta 22 noviembre 2017 en http://oiprodat.com/2015/09/14/la-proteccion-de-datos-geneticos-y-su-impacto-en-los-derecho-humanos/.

CIFUENTES, S. E., *Derechos personalísimos*, 3a. ed. actualizada y ampliada, Editorial Astrea de A. y R. Depalma, Ciudad de Buenos Aires, 2008.

COMISIÓN DE LA CONSTITUCIÓN DE ECUADOR DE 1967, [Acta No. 152].

COMISIÓN DE LA CONSTITUCIÓN DE ECUADOR DE 1967, [Acta No. 154].

COMISIÓN DE LA CONSTITUCIÓN DE ECUADOR DE 1967, [Acta No. 155].

CONDE ORTIZ, C., *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*, Dykinson, Madrid, 2005.

CONGRESO NACIONAL DEL ECUADOR, [Código de la Niñez y Adolescencia. Ley 100. Registro Oficial No. 737, de 03 de enero de 2003], *Lexis Ecuador*, fecha de consulta 2 junio 2017, en www.lexis.com.ec.

CONGRESO NACIONAL DEL ECUADOR, [Ley Orgánica de Donación y Trasplante de órganos, tejidos y células, Ley 0, Registro Oficial No. 398, de 04 de marzo de 2011.], *Lexis Ecuador*, fecha de consulta 22 noviembre 2017, en www.silec.com.ec.

CONGRESO NACIONAL DEL ECUADOR, [Ley Orgánica de la Defensoría del Pueblo, Ley 1. Registro Oficial No. 7, de 20 de febrero de 1997], *Lexis Ecuador*, fecha de consulta 22 noviembre 2017, en www.silec.com.ec.

CONGRESO NACIONAL DEL ECUADOR, [Ley Orgánica de Transparencia y acceso a la Información Pública, Ley 24. Registro Oficial suplemento No. 337, de 18 de mayo de 2004], *Lexis Ecuador*, fecha de consulta 22 noviembre 2017, en www.silec.com.ec.

CONGRESO NACIONAL DEL ECUADOR 1994, [Acta No. 2 A].

CONGRESO NACIONAL DEL ECUADOR DE 1995, [Acta No. 1.

CONSEJO DE EUROPA, [Convenio N^{o} 108 del Consejo de Europa, de 28 de Enero de 1981, para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal].

CONSEJO DE EUROPA, [Recomendación N^{o} R(97) 18 y exposición de motivos del comité de ministros a los estados miembros relativa a la protección de datos de carácter personal, recogidos y tratados con fines estadísticos].

CORTE CONSTITUCIONAL DEL ECUADOR, *Protocolo para la Elaboración de Precedentes Constitucionales Obligatorios*, Resolución No. 4 - RA 2010 (5 de agosto de 2010).

CORTE CONSTITUCIONAL DE COLOMBIA, [Sentencia C-748/11], fecha de consulta 26 mayo 2017, en http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm.

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0039-2007-HD], ROS, No. 133 (10 de julio de 2009).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0044-2007-HD], ROS No. 137, (4 de agosto de 2009).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0013-08-HD], ROS, No. 127 (15 de junio de 2009

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0022-2008-HD], ROS, No. 133 (10 de julio de 2009)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0023-2008-HD], ROS No. 518, (30 de Enero de 2009).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0044-2008-HD], en ROS, No. 87 (11 de diciembre de 2008

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0066-08-HD], en ROS, No. 135 (17 de julio de 2009.

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0079-2008-HD], en ROS, No. 8 (4 de septiembre de 2009).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 068-10-SEP-CC], ROS No. 372, (27 de enero de 2011).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0070-2008-HD], ROS, NO. 2 (20 de agosto del 2009)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0001-11-HD], en ROSEC, No. 7, (2 de mayo de 2017).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 001-2014-PJO-CC], ROS No. 281, (3 de julio de 2014).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0002-14-HD], ROEC, No. 2 (5 de junio de 2017)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 175-14-SEP-CC], ROEC, No. 406 (30 de diciembre de 2014)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 001-14-PJO-CC], en ROS, No. 281 (2 de julio de 2014).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0001-15-11D], ROEC, No. 70 (29 de marzo de 2019)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 007-15-SIS-CC], en ROS, No. 472, (02 de abril de 2015).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 025-15-SEP-CC], ROS No. 485, (22 de Abril 2015).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 032-15-SEP-CC], ROS No. 462, (19 de Marzo de 2015).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No.182-15-SEP-CC], ROS No. 596, 28 de septiembre de 2015).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0001-16-HD], ROEC No. 1 (20 de marzo de 2017)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 008-16-SIS-CC], ROS No. 767 (2 de junio de 2016)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 048-16-SIS-CC], ROS No. 878 (10 de noviembre de 2016)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 386-16-SEP-CC], ROEE No. 852 (24 de enero de 2017)

CORTE CONSTITUCIONAL, [Sentencia No. 1-17-HD], ROEC No. 70 (29 de marzo de 2019)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 006-17-SCN-CC], en ROEC, No. 22 (05 de diciembre de 2017).

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 008-17-SIS-CC], ROEC No. 7 (2 de mayo de 2017)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 026-17-SIN-CC], ROEC No. 22 (5 de diciembre de 2017)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 046-17-SIS-CC], ROEC No. 77 (26 de abril de 2019)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 131-17-SEP-CC], ROEC No. 6 (3 de julio de 2017)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 312-17-SEP-CC], ROEC No. 22 (05 de diciembre de 2017)

CORTE CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 042-18-SIS-CC 42], ROEC No. 62 (19 de octubre de 2018)

CORTE CONSTITUCIONAL DEL ECUADOR PARA EL PERÍODO DE TRANSICIÓN, [Sentencia No. 012-2009-SEP-CC].

CORTE CONSTITUCIONAL DEL ECUADOR PARA EL PERÍODO DE TRANSICIÓN, [Sentencia No. 019-09-SEP-CC2], en ROS, No.018 (3 de septiembre de 2009).

CORTE CONSTITUCIONAL DEL ECUADOR PARA EL PERÍODO DE TRANSICIÓN, [Sentencia No. 068-2010-SEP-CC].

CORTE CONSTITUCIONAL DEL ECUADOR PARA EL PERÍODO DE TRANSICIÓN, [Sentencia No. 0074-2008-HD]

CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso Acosta Calderón Vs. Ecuador].

CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso Blanco Romero y Otros Vs. Venezuela].

CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso García Asto y Ramírez Rojas].

CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso Gómez Palomino Vs. Perú].

CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso Gutiérrez Soler Vs. Colombia].

CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso "Masacre de Mapiripán" Vs. Colombia].

CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso Raxcacó Reyes Vs. Guatemala].

CORTE INTERAMERICANA DE DERECHOS HUMANOS, [Caso Yatama Vs. Nicaragua].

CRUZ VILLALÓN, PEDRO, "Formación y evolución de los derechos fundamentales", *Revista Española de Derecho Constitucional*, vol. 25, 1989.

DAVARA FERNÁNDEZ DE MARCOS, I., *Hacia la estandarización de la protección de datos personales: propuesta sobre una «tercera vía o tertium genus» internacional*, 1a. ed, La Ley, Las Rozas, Madrid, 2011.

DAVARA RODRÍGUEZ, M. Á., *Manual de derecho informático*, Thomson Aranzadi, Cizur Menor, 2015.

DE LA PARRA TRUJILLO, E., "Los derechos de la personalidad: Teoría General y su distinción con los derechos humanos y las garantías individuales", *Jurídica. Anuario del Departamento de Derecho de la Universidad Iberoamericana*, vol. No. 31, 2001, fecha de consulta 03 octubre 2017, https://revistas-colaboracion.juridicas.unam.mx/index.php/juridica/article/view/11436/10481

DIRECTIVA 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, Luxemburgo

DUASO CALÉS, ROSARIO, "Regulación Europea sobre difusión de la jurisprudencia en internet", en *Buenas Prácticas para la implementación de soluciones tecnológicas en la administración de justicia*, IIJusticia, Instituto de Investigación para la Justicia, México, 2011, fecha de consulta 22 noviembre 2017, en http://www.iijusticia.org/heredia/PDF/Duaso.pdf.

ECHEVERRÍA, JULIO, "El Estado en la Nueva Constitución", en *La Nueva Constitución del Ecuador. Estado, derechos e instituciones*, Corporación Editora Nacional, Quito, 2009 (Estudios Jurídicos).

ECUADOR, "Secretaria Nacional de Planificación y Desarrollo - Senplades 2013".

ENCABO VERA MIGUEL ÁNGEL, *Derechos de la personalidad*, Marcial Pons, Madrid, 2012.

ESPAÑA, "Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.".

España: LEY ORGÁNICA 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales LOPD-GDD

FERNÁNDEZ ESTEBAN, M. L., *Nuevas tecnologías, Internet y derechos fundamentales*, MacGraw-Hill, Madrid, 1998.

FERRAJOLI, LUIGI, *Derechos y garantías: La ley del más débil*, cuarta, Editorial Trotta, Fernandez, 2004.

G29, "Dictamen 4/2007 Sobre el concepto de datos personales".

GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales: en la Era del Big Data y de la computación ubicua*, Dykinson, Madrid, 2016.

GHERSI, C. A., *Derecho civil: parte general*, 3a. ed. actualizada y ampliada, Editorial Astrea de Alfredo y Ricardo DePalma, Ciudad de Buenos Aires, 2002.

GOIG MARTÍNEZ, JUAN MANUEL; NUÑEZ MARTÍNEZ, MARÍA ACRACIA; NUÑEZ RIVERO, CAYETANO, *El sistema constitucional de derechos y libertades según la jurisprudencia del Tribunal Constitucional*, Editorial Universitas Internacional S.L., Madrid, 2006.

GOZAÍNI, O. A., *Hábeas data: protección de datos personales: doctrina y jurisprudencia*, Rubinzal-Culzoni Editores, Buenos Aires, 2001.

GRAN SALA DEL TRIBUNAL CONSTITUCIONAL ALEMÁN, "Sentencia Von Hannover c. Alemania".

GRIJALVA, AGUSTÍN, "Interpretación constitucional, jurisdicción ordinaria y Corte Constitucional", Corporación Editora Nacional, 2009 (Estudios Jurídicos).

GRIJALVA JIMÉNEZ, AGUSTÍN, *Constitucionalismo en Ecuador*, Corte Constitucional para el Período de Transición, Quito, 2012.

GUTIÉRREZ GUTIÉRREZ, I., *Dignidad de la persona y derechos fundamentales*, M. Pons, Ediciones Jurídicas y Sociales, Madrid [Spain], 2005.

HABERLE, PETER, *La garantía del contenido esencial de los derechos fundamentales en la ley fundamental de Bonn*, Dykinson, Madrid, 2003.

HERRÁN ORTÍZ, A. I., *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales*, Dykinson, Madrid, 2002.

LARREA HOLGUÍN, J., *Derecho constitucional ecuatoriano*, 1. ed, Corporación de Estudios y Publicaciones, Quito, Ecuador, 2000.

LARREA HOLGUÍN, J., *Derecho constitucional ecuatoriano*, Corporación de Estudios y Publicaciones, Quito, Ecuador, 2000.

LASARTE ÁLVAREZ, C., *Principios de derecho civil. Tomo primero, Tomo primero,* Marcial Pons, Madrid [etc., 2016.

MARÍA MOLINA CRESPO, PRESIDENTA LA MESA 1 DE LA CONSTITUYENTE DE 2008, "Informe de la Mesa 1 sobre artículos aprobados para que sean sujetos a discusión de la Asamblea Constituyente de Ecuador de 2008 sobre Derechos Civiles, debido proceso, Derechos Políticos y Derecho a la Comunicación".

MEDINA GUERRERO, M., *La protección constitucional de la intimidad frente a los medios de comunicación*, Tirant lo Blanch, Valencia, 2005.

MURILLO DE LA CUEVA, P. L., "El Derecho a la autodeterminación informativa".

NINO, C. S., *Fundamentos de derecho constitucional: análisis filosófico, jurídico y politológico de la práctica constitucional*, Editorial Astrea De A. y R. Depalma, Buenos Aires, 1992.

NOGUEIRA ALCALÁ, HUMBERTO, "Aspectos de una teoría de los derechos fundamentales: la delimitación, regulación, garantías y limitaciones de los derechos fundamentales.", *Revista Electrónica Ius et Praxis*, vol. 11, n.º 2, 2005, (Talca), fecha de consulta 22 noviembre 2017, en www.scielo.cl/iusetp.htm.

OSSORIO Y FLORIT, MANUEL, *Enciclopedia Jurídica Omeba*, vol. XIV, Omeba.

PARDINI, ANIBAL, "La información y su sistema de protección", *DeCITA 5/6.2006 Revista de direito do comércio internacional temas e atualidades Internet, comércio eletrônico e sociedade da informação*, vol. 5/6, 2006.

PÉREZ LUÑO, A. E., *Derechos humanos, estado de derecho y constitución*, 7. ed, Tecnos, Madrid, 2001.

PISARELLO, GERARDO, *Un largo termidor: historia y crítica del constitucionalismo antidemocrático*, Corte Constitucional para el Período de Transición, Quito, 2011.

PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR, "Reglamento a la Ley de Comercio Electrónico. DEJ 3496. Registro Oficial No. 735 de 31 de diciembre de 2002", *Lexis Ecuador*, fecha de consulta 22 noviembre 2017, en www.silec.com.ec.

PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR, "Reglamento a Ley del Sistema Nacional de Registro de Datos Públicos en la Disposición General Séptima DEJ 950 - RS 718 - 23/mar./2016", *Lexis Ecuador*, fecha de consulta 22 noviembre 2017, en www.silec.com.ec.

PRIETO SANCHIS, L., *Justicia constitucional y derechos fundamentales*, Trotta, Madrid, 2009.

PRIETO SANCHÍS, LUIS, "La limitación de los derechos fundamentales y la norma de clausura del sistema de libertades", *Derechos y libertades: revista del Instituto Bartolomé de las Casas*, vol. No. 8, 2000.

PUCCINELLI OSCAR R., "Tipos y subtipos de hábeas data en América latina", fecha de consulta en 22 noviembre 2017, http://www.iprofesional.com/adjuntos/documentos/08/0000887.pdf.

REYES AMÁN, JONNATHAN, "Derecho a la protección de datos personales en las bases de datos judiciales accesibles al público en temas de niñez y adolescencia".

RIVERA, JULIO, *Instituciones del Derecho Civil*, vol. II, Abeledo Perrot, 1992.

RODRÍGUEZ VILLAFAÑEZ, MIGUEL JULIO, "La transparencia en el Poder Judicial de Argentina, Reforma Judicial", *Reforma Judicial, Revista Mexicana de Justicia*, vol. 2, 2003, pp. 163-193, fecha de consulta 23 agosto 2016, en http://revistas.juridicas.unam.mx/index.php/reforma-judicial/article/view/8567/10590.

ROMERO COLOMA, A. M., *Los bienes y derechos de la personalidad*, 1a ed, Trivium, Madrid, 1985.

SALGADO PESANTES, HERNÁN, *Lecciones de Derecho Constitucional*, Ediciones Legales S.A., Quito, Ecuador, 2012.

SÁNCHEZ BRAVO, A. A., *La protección del derecho a la libertad informática en la Unión Europea*, Universidad de Sevilla, Secretariado de Publicaciones, Sevilla, 1998.

SANTOS GARCÍA, D., *Nociones generales de la Ley orgánica de protección de datos y su reglamento: adaptado al RD 1.720/2007 de 21 de diciembre*, 2. ed, Tecnos, Madrid, 2012.

SERRANO PÉREZ, M. M., *El derecho fundamental a la protección de datos: derecho español y comparado*, 1. ed, Civitas, Madrid [Spain], 2003.

STORINI, CLAUDIA, "Las garantías constitucionales de los Derechos Fundamentales en la Constitución Ecuatoriana de 2008", en *La Nueva Constitución del Ecuador. Estado, derechos e instituciones*, Corporación Editora Nacional, Quito, Ecuador, 2009 (Estudios Jurídicos).

SUÁREZ SALAZAR,EMILIO ESTEBAN, "Distorsiones del sistema de selección y revisión de sentencias de la Corte Constitucional Ecuatoriana", 2015, Universidad Andina Simón Bolívar, Quito, Ecuador.

SUBIZA PÉREZ, I.; ARIAS POU, M., *La protección de datos y sus mundos*, DAPP, Pamplona, 2009.

TOBAR DONOSO, JULIO; LARREA HOLGUIN, JUAN, *Derecho Constitucional ecuatoriano*, Cuarta, Corporación de Estudios y Publicaciones, Quito, Ecuador, 1996.

TORRES, LUIS FERNANDO, "El presidencialismo constituyente y el Estado constitucional de Montecristi", en *La Nueva Constitución del Ecuador. Estado, derechos e instituciones*, Corporación Editora Nacional, Quito, 2009 (Estudios Jurídicos).

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [SSTC 105/90].

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 11/1981].

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 12/2012].

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 57/1984].

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 73/1982].

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 81/2001].

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 117/1994].

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 120/1990].

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 134/1999].

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 139/1995].

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 139/2007].

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, [STC 231/1988].

TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 021-HD-IS].

TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0046-2002-HD].

TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0022-2004-HD].

TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0033-2004-HD].

TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0007-2006-HD].

TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0015-2006-HD].

TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0034-2006-HD]

TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0039-2008-HD].

TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0042-2005-HD].

TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0068-08-CC].

TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0070-2003-HD].

TRIBUNAL CONSTITUCIONAL DEL ECUADOR, [Sentencia No. 0102-2004-HC].

TRONCOSO REIGADA, A., *La Protección de datos personales: en busca del equilibrio*, Tirant lo Blanch, Valencia, 2010.

TRUJILLO, J. C.; AVILA SANTAMARÍA, R., "Los Derechos en el Proyecto de Constitución", en *Análisis nueva constitución*, ILDIS, Friedrich Ebert Stiftung : La Tendencia, Quito, 2008.

UPRIMNY YEPES, RODRIGO, "Reflexiones tentativas sobre Constitución, economía y justicia constitucional en América Latina", en *Genealogía de la justicia constitucional ecuatoriana*, Corte Constitucional para el Período de Transición, Quito, 2011.

VALENCIA ZEA, A., *Derecho civil*, vol. I, Temis, Bogotá, 1966.

VEGA VEGA, J. A., *Derecho mercantil electrónico.*, Editorial Reus, Madrid, 2015, fecha de consulta 6 enero 2017, en http://public.eblib.com/choice/publicfullrecord.aspx?p=4569794.

VIDAL MARÍN TOMÁS, *El derecho al honor y su protección desde la Constitución Española*, Centro de Estudios Políticos y Constitucionales y Boletín Oficial del Estado, Madrid, 2000.

VILLASAU SOLANA, M.; VILA MUNTAL, M. Á., "Intimidad y datos personales en Internet", en Miquel Peguera Poch (ed.) *Principios de derecho de la sociedad de la información*, Thomson Reuters-Aranzadi, Cizur Menor (Navarra, 2010.

ZABÍA DE LA MATA, J.; AGÚNDEZ LERÍA, I. M. (eds.), *Protección de datos: comentarios al reglamento*, 1a ed., Editorial Lex Nova, Valladolid, 2008.

ZAGREBELSKY, GUSTAVO, *El derecho dúctil*, novena, Editorial Trotta, Fernandez, 2009.

ZAMBRANO ALVAREZ, DIEGO, "Jurisprudencia vinculante y precedente constitucional", en *Apuntes de Derechos Procesal Constitucional*, Centro de Estudios y Difusión del Derecho Constitucional, Quito, Ecuador, 2011.

ANEXO 1

1. METODOLOGÍA DE INVESTIGACIÓN.

TÍTULO DEL PROYECTO DE INVESTIGACIÓN
La aplicación del derecho a la protección de datos y del hábeas data en la jurisprudencia constitucional. Desde 1993 al 2014.

DATOS DEL INVESTIGADOR PRINCIPAL (IP) O DIRECTOR DEL PROYECTO	
Nombre y apellidos	*Lorena Naranjo Godoy*
Institución a la que pertenece	*UDLA*
Cargo y categoría científica	*Docente Investigador*
Carrera y Facultad	*Derecho*

DATOS GENERALES

TIPOLOGÍA DEL PROYECTO (Si aplica puede marcar más de una opción)	**CATEGORÍA DEL PROYECTO** (por favor seleccione solo una)
Investigación Básica: X Investigación Aplicada: ___ Desarrollo Tecnológico: ___	Primera aplicación: X Renovación: ___

LÍNEAS DE INVESTIGACIÓN QUE TENDRÁ IMPACTO EL PROYECTO (Si aplica puede marcar más de una opción)	
Salud y Bienestar	☐
Educación	☐
Comunicación y tecnología	☒
Sociedad, Comunidad y Cultura	☐
Hábitat, biodiversidad y patrimonios	☐

RESUMEN DEL PROYECTO (Máximo 250 palabras)

A nivel normativo constitucional el hábeas data en el Ecuador es una garantía del derecho a la protección de datos, que no se limita a la eliminación, actualización o rectificación sino a verificar que estos datos no hayan sido utilizados como mecanismos de discriminación, ya sea a través de valoraciones equivocadas de datos o por uso ilegítimo. La normativa ecuatoriana supera el contenido tradicional de hábeas data y establece no solo su carácter informativo, aditivo, rectificador y correctivo, exclutorio, cancelatorio, entre otros, sino su finalidad reparadora, que pretende evitar potenciales, existentes o futuros daños no solo con la supresión, eliminación, cancelación del dato sino la corrección de actos discriminatorios. La Ley Orgánica de Garantías Jurisdiccionales, en su Art. 49 señala que la acción de hábeas data reconoce la reparación integral. Como vemos a nivel normativo el Ecuador está a la vanguardia en el contenido normativo del derecho a la protección de datos personales, sin embargo es necesario verificar la línea jurisprudencial constitucional, a fin de determinar si los tribunales han logrado aplicar las distintas dimensiones del derecho a la protección de datos, relativo no solo a la autodeterminación informativa, a la cancelación, corrección y actualización de los datos sino sobre todo a la eliminación a título de reparación integral, de todas aquellas consecuencias dañosas y discriminatorias provenientes de la utilización de datos. El objetivo de esta investigación es determinar la aplicación del derecho a la protección de datos y del hábeas data en la jurisprudencia constitucional, desde 1993 al 2014.

Autodeterminación informativa, hábeas data, jurisprudencia relevante, protección de datos, reparación integral.

TIEMPO DE EJECUCIÓN DEL PROYECTO	
DURACIÓN DEL PROYECTO EN MESES (DE 6 A 18 MESES)	**12**

A. LOCALIZACIÓN GEOGRÁFICA DEL PROGRAMA Y/O PROYECTO

COBERTURA DE EJECUCIÓN DEL PROGRMA Y/O PROYECTO (SELECCIONE ÚNICAMENTE UN TIPO DE COBERTURA)		
NACIONAL ☐		
ZONAS DE PLANIFICACIÓN	**ZONA 1 (CARCHI, ESMERALDAS, IMBABURA Y SUCUMBÍOS)** **ZONA 2 (NAPO, ORELLANA Y PICHINCHA)** **ZONA 3 (CHIMBORAZO, COTOPAXI, PASTAZA Y TUNGURAHUA)** **ZONA 4 (MANABÍ, STO. DOMINGO DE LOS TSÁCHILAS)** **ZONA 5 (BOLÍVAR, GUAYAS, LOS RÍOS Y SANTA ELENA)** **ZONA 6 (AZUAY, CAÑAR Y MORONA SANTIAGO)** **ZONA 7 (EL ORO, LOJA Y ZAMORA CHINCHIPE)** **ZONA 8 (CANTONES GUAYAQUIL, SAMBORONDÓN, DURÁN)** **ZONA 9 (DISTRITO METROPOLITANO DE QUITO)**	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☒
PROVINCIAL ☐	**PICHINCHA**	
LOCAL ☒	**QUITO**	

B. PERSONAL DEL PROYECTO

Puede adicionar más filas en caso que necesite

Función en el proyecto	Nombre completo	Entidad a la que pertenece	Cargo /función
Director del proyecto (Completar anexo 1)	Lorena Naranjo Godoy	UDLA	Docente a tiempo completo
Coordinadora	Daniela Macías	UDLA	Tesista
Derecho Informático, Der 903-2 del período académico 2015-1, septiembre de 2014 hasta febrero de 2015	Alumnos DER903-2	UDLA	Alumnos

C. DESCRIPCIÓN DEL PROYECTO

PLANTEAMIENTO DEL PROBLEMA Y JUSTIFICACIÓN DEL PROYECTO
(máximo de 500 palabras o una cuartilla)

El Ecuador está a la vanguardia en el contenido normativo pues consagra a nivel constitucional el derecho a la protección de datos personales, además establece la acción constitucional denominada hábeas data para exigir su cumplimiento.

La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, por su parte consagra una característica diferenciadora que supera a otras legislaciones, esto es el hábeas data reparador. Es decir, no solo establece su carácter informativo, aditivo, rectificador y correctivo, exclutorio, cancelatorio, entre otros, sino su finalidad reparadora, que pretende evitar potenciales, existentes o futuros daños no solo con la supresión, eliminación, cancelación del dato sino la corrección de actos discriminatorios.

Si bien a nivel normativo el Ecuador está a la vanguardia en el desarrollo normativo, sin embargo es necesario verificar su línea jurisprudencial, a fin de determinar si los tribunales han logrado aplicar las distintas dimensiones del derecho a la protección de datos, relativo no solo a la autodeterminación informativa, sino sobre todo a la eliminación a título de reparación integral, de todas aquellas consecuencias dañosas y discriminatorias provenientes de la utilización de datos.

La jurisprudencia es una de las fuentes del derecho que permite verificar como se está aplicando el derecho en una sociedad, en este caso vamos a verificar cómo se está aplicando la normativa relativa al derecho a la protección de datos y al hábeas data en los casos que ha tenido conocimiento la Corte Constitucional del Ecuador desde 1993 hasta el 2014.

Como se trata de una contrastación de la realidad versus la normativa invocada por los abogados defensores y aplicada por los tribunales, es indispensable una correcta identificación de los hechos que motivaron la solicitud de la acción de hábeas data y los argumentos y motivaciones que permiten resolver los casos planteados. El análisis jurisprudencial, es entonces, el mecanismo que permite visibilizar la problemática planteada, es decir que pese a la existencia de una adecuada normativa constitucional y legal nuestros tribunales aun dictan sentencias apegadas al anterior sistema de protección de datos asociado a la intimidad.

Es importante el parámetro de tiempo por cuanto permite verificar el cambio que se ha producido durante este periodo. Anotándose que, para el análisis debemos tomar en cuenta la Constitución del 2008 es la primera que reconoce y positiviza el derecho a la protección de datos, las anteriores constituciones establecían únicamente el hábeas data.

OBJETIVO GENERAL DEL PROYECTO

Determinar cuál es la aplicación del derecho a la protección de datos y del hábeas data en la jurisprudencia constitucional, desde 1993 al 2014, en Ecuador.

OBJETIVOS ESPECÍFICOS

1. Buscar y seleccionar información útil y relevante para el proyecto de investigación (jurisprudencia).
2. Organizar y sistematizar las resoluciones dictadas por la Corte Constitucional del Ecuador desde 1993 hasta el 2014 relativas a Hábeas Data y Protección de Datos Personales.
3. Elaborar fichas de resumen para tabulación de datos y determinación de las corrientes jurisprudenciales.
4. Crear un TESAURO de términos básicos para la sistematización de la información.
5. Elaborar un informe final escrito que contenga las conclusiones de la investigación y recomendaciones de la investigación.

METODOLOGÍA
(Mínimo de 500 palabras y máximo de 2 cuartillas)

El trabajo de investigación será realizado por el grupo de estudiantes del semestre septiembre 2014 a febrero 2015 de la materia de Derecho Informático, código DER903-2 de la Facultad de Derecho. Este proyecto de investigación será valorado dentro de un porcentaje para el progreso 1, progreso 2 y evaluación final.

Para el desarrollo de este proyecto de investigación es indispensable que los estudiantes y los miembros del equipo aprendan a procesar jurisprudencia.

Con esta finalidad es necesario comprender ciertos criterios generales como: **SISTEMA =** Conjunto de reglas o principios sobre una materia racionalmente enlazados entre sí. Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto.

PRIMERA: I. Recopilación, Registro o Archivo de la Información:

PRIMERA: I. Recopilación, Registro o Archivo de la Información:

- Ubicación de los fallos íntegros a ser procesados en las respectivas Salas de la Corte Constitucional del año de su responsabilidad.
    - La sentencia o auto deben estar completos, incluidos los autos que los aclaren, amplíen o reformen, respectivamente y los votos salvados de ser el caso que también deben procesarse.
    - Deben identificarse en forma particular, para ello se deben establecer los siguientes datos**:** No. de expediente Corte Constitucional, juzgado de procedencia, tipo de acción, pronunciamiento, Juez de primer nivel, Juez de apelación, pronunciamiento constitucional, accionante: natural, individual, femenino, accionado: jurídico, privado.
- Obtención de las reproducciones fidedignas y oficiales de los fallos ubicados:
    - La mayoría de los fallos consta en la base de datos que se ha compartido a los estudiantes.
    - Sin embargo, si no existen datos completos en la base de datos, o estos se encuentran incompletos o fraccionados es necesaria la obtención de la información de los procesos físicos para lo cual es indispensable copias simples en buen estado, ejemplar de la publicación en el Registro Oficial que puede ser obtenida de LEXIS por ejemplo, repertorios de jurisprudencia, rendiciones de cuentas y otros documentos oficiales).

SEGUNDA: II. Digitalización de los documentos obtenidos.

- Transcripción de las copias simples de ser el caso o copia digital si se ha obtenido la información de fuentes digitales e incorporación en la base de datos general que ha sido compartida con los estudiantes. Esto solo opera si no existe el texto en la base de datos general.
- Almacenamiento de la información en los directorios, las carpetas o subcarpetas informáticas correspondiente al año específico de su responsabilidad.
- Como los archivos son compartidos se les solicita cuidado y meticulosidad en el manejo de la información para no perjudicar el trabajo de sus compañeros.

TERCERA: III. Sistematización de los Datos Almacenados. Elaboración de Tesauros y Abstracts o breves resúmenes.

- **TESAURO =** neo latín thesaurus = tesoro, tesorería. Listado de palabras o términos empleados para representar conceptos. Es una herramienta de control terminológico, llamado también sistema de vocabulario controlado y dinámico o sistema de indización controlado, que establece relaciones entre los distintos términos contenidos en él y se aplica a un campo específico del conocimiento. El lenguaje utilizado en los tesauros se conoce como lenguaje documentario o lenguaje de información y los términos que contiene se llaman descriptores.

- Los términos que conforman el tesauro se interrelacionan entre ellos bajo tres modalidades de relación:
    - **Relaciones jerárquicas**: Establece subdivisiones que generalmente reflejan estructuras de TODO/Parte. Ejem. CONTRATO/Compraventa**.**
    - **Relaciones de equivalencia**: Controla la Sinonimia, Homonimia y Antonimia entre los términos. Ejem. Préstamo de Uso. Ver Comodato**.**
    - **Relaciones asociativas**: Mejoran las estrategias de recuperación y ayudan a reducir la polijerarquia entre los términos. Es un intermedio entre el lenguaje natural y el lenguaje jurídico. Ejem. Rechazo momentáneo de la petición del actor. Ver Sentencia Inhibitoria.
- Debe existir un orden en la ubicación de términos en las relaciones escogidas, así se debe establecer en forma alfabética, temática y jerárquica dentro de cada relación**.** Debe existir un orden en la ubicación de términos en las relaciones escogidas, así se debe establecer en forma alfabética, temática y jerárquica dentro de cada relación.
- La relación debe ser ascendente o descendente entre términos genéricos, particulares y específicos. La relación puede ser además a priori, según el tema que representan, o a posteriori, de acuerdo con el contenido de la información que se asocia a ellos, el desarrollo y los cambios jurisprudenciales, legislativos y doctrinales**.**
- El tesauro es un producto independiente de cada grupo según sus propios resultados de investigación pero debe ser parte de un tesauro global de tal manera que todos los grupos trabajen sobre los mismos términos. No se admitirán tesauros repetidos entre grupos, el incumplimiento de esta disposición inhabilita la presentación de esta parte del trabajo de investigación e impide la presentación del resto del portafolio hasta que no se corrijan los errores.

¿Cómo se elabora un tesauro?

- **En primer lugar** se identifica un TEMA O DESCRIPTOR: Los temas o descriptores son términos de indización (hacer índices), términos autorizados o términos preferidos; representan un concepto en forma de sustantivo o frase sustantiva. “palabras claves autorizadas”. Es todo concepto o término jurídico que tenga autonomía conceptual y por ello sea distinto o diferenciado de otros conceptos del Derecho. Puede ser simple o compuesto, según esté formado por una o varias palabras**.** Dentro de cada descriptor (Término Genérico) pueden haber otros descriptores (Término Particular).
- **En segundo lugar** se identifica el SUBTEMA O RESTRICTOR: Son palabras o frases que orientan al investigador sobre el tema o aspecto específico al que se refiere la información o documento. Están asociados al descriptor y funcionan como subtítulos que guían y restringen la búsqueda**.**

ABSTRACT= Es un breve, apropiado y comprensivo resumen de un artículo contenido académico o científico. Si bien el abstract se ubica al inicio del procesamiento debería ser la última sección que se escribe. El abstract debe guardar la misma estructura del resto del texto. El

abstract debe ser tan conciso y concreto que le permita al lector leer o no el contenido completo de la sentencia.

Para facilitar este trabajo se ha envía a cada uno de los estudiantes un formulario elaborado en google drive, que consiste en una ficha que debe ser llenada con absoluto cuidado y dedicación pues de este trabajo dependen su análisis y conclusiones al final del proceso de investigación.

Posteriormente, la coordinadora debe revisar el trabajo de los estudiantes para verificar su confiabilidad. Finalmente, la investigadora principal revisa nuevamente la selección, organización y procesamiento de la jurisprudencia para que las conclusiones sean correctas.

RESULTADOS ESPERADOS
(máximo de 200 palabras)

La jurisprudencia como fuente principal y directa del derecho, ha dejado de ser una compleja recopilación de fallos, para constituirse a la luz de los nuevos textos y principios constitucionales en el mayor y más amplio referente jurídico para la cabal aplicación del texto normativo. Pero esta amplitud, no solo está asociada a su gran aceptación, sino a las casuísticas tratadas y puntos de derecho sobre los cuales ha debido decidir, que por su extensión y comprensión lógico jurídica, requieren de un manejo especializado que permita aprovechar exponencialmente sus virtudes.

Sin embargo, los tribunales no siempre aplican un derecho en su contenido y dimensiones complejas y completas, es por ello que resulta fundamental el análisis de la línea jurisprudencial y del tratamiento que la Corte Constitucional ha realizado sobre ciertos temas jurídicos.

Esta revisión de la actuación jurisprudencial tiene como finalidad identificar la línea de evolución jurisprudencial sobre el derecho a la protección de datos personales y el hábeas data y determinar si existe un avance en la comprensión de este derecho y garantía constitucional o si por el contrario se evidencia una falta de comprensión y conocimiento sobre los alcances de estas normativas.

Para conseguir este objetivo es fundamental aprender a procesar jurisprudencia. Esta experticia debe ser parte de las competencias y destrezas que se deben desarrollar en los alumnos de derecho y tesista, pues desde la vigencia de la Constitución del 2008 que se consagra como fuente de derecho fundamental la jurisprudencia, es indispensable aprender a identificar, organizar, comprender, procesar y analizar la jurisprudencia ecuatoriana.

El producto final a entregarse será un informe final escrito de las conclusiones y recomendaciones de la investigación, junto con un portafolio que contiene las sentencias seleccionadas y organizadas, las bases de datos de procesamiento de jurisprudencia y el tesauro.

El proyecto resulta importante y novedoso por la participación crítica de estudiantes de derecho en su elaboración, ya que desde las aulas analizan las sentencias del más alto tribunal.

Esta investigación y otras que pudieran desprenderse con la misma metodología, pretenden convertirse en mecanismo eficiente para evaluación de la calidad de las resoluciones judiciales, ya que el estudio de la motivación de las sentencias permite analizar los criterios jurídicos utilizados para la resolución de los diversos casos prácticos, revisión que se convierten en garantía de imparcialidad y justicia.

GESTIÓN POR RESULTADOS DEL PROYECTO

Objetivos específicos	Resultado esperado	Indicador	Medio de Verificación
Buscar y seleccionar información útil y relevante para el proyecto de investigación (jurisprudencia).	Agotamiento de fuentes.	Revisar el 100% de las sentencias dictadas por la Corte Constitucional relativas al tema de investigación durante dos meses.	Contrastación del número de sentencias dictadas por la Corte Constitucional versus el número de resoluciones buscadas y seleccionadas.
Organizar y sistematizar las resoluciones dictadas por la Corte	Tener información para establecer una línea de evolución	En el primer mes 200 resoluciones seleccionadas y	Base de datos en Excel que contiene las sentencias seleccionadas

Constitucional.	jurisprudencial.	organizadas para su análisis.	organizadas, de contenido completo y en versión digital.
Elaborar fichas de resumen para tabulación de datos y determinación de las corrientes jurisprudenciales.	Establecer una línea de evolución jurisprudencial.	En el primer mes 100 fichas de procesamiento. En el segundo mes 100 fichas de procesamiento.	Base de datos en Excel que contiene la totalidad de las fichas de procesamiento.
Crear un TESAURO de términos básicos para la sistematización de la información.	Reporte de tesauro completo y revisado.	En el primer mes se cruzará información de 100 fichas de procesamiento para la elaboración del Tesauro. En el segundo mes se cruzará información de 100 fichas de procesamiento para la elaboración del Tesauro.	Base de datos en Excel que contiene el reporte de tesauro.
Elaborar un informe final escrito que contenga las conclusiones de la investigación y recomendaciones de la investigación.	Informe completo, finalizado y revisado.	Se revisarán 200 sentencias que fueron procesadas.	Portafolio que contiene las sentencias seleccionadas y organizadas, las bases de datos de procesamiento de jurisprudencia y tesauro y el informe final.

BENEFICIOS DEL PROYECTO			
Beneficios científicos-tecnológicos	**Beneficios económicos**	**Beneficios sociales o ambientales**	**Entregables**
		Desarrollo de destrezas y competencias en los estudiantes de derecho respecto del manejo y procesamiento de jurisprudencia, indispensable en el estado actual del derecho en el los precedentes jurisprudenciales son fuente obligatoria.	Evaluación de los estudiantes a través de un porcentaje del progreso 1, progreso 2 del curso del presente semestre de DER903-2
		Participación crítica de estudiantes de derecho, que desde las aulas analizan las sentencias del más alto tribunal de justicia constitucional.	Informes final para evaluación final del curso del presente semestre de DER903-2
		Investigación que pretende convertirse en mecanismo eficiente para evaluación de la calidad y motivación de las resoluciones judiciales como garantía de imparcialidad y	Informe final formará parte de la tesis doctoral de la investigadora principal.

		justicia.	

D. CRONOGRAMA DE ACTIVIDADES POR AÑO DEL PROYECTO

Las principales actividades que componen el cronograma generalmente son:

(I) planificación
(II) ejecución, siguiendo la metodología previamente descrita,
(III) análisis de resultados,
(IV) redacción del artículo y documento final de presentación,
(V) divulgación de resultados.

Estas actividades principales a su vez pueden estar compuestas de actividades derivadas de éstas. Para la construcción del diagrama de Gantt evitar un orden seriado de las actividades; planifique actividades en paralelo.

AÑO 1			**MESES**												
Ítem	***Actividades o tareas***	***Investigador Responsable***	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***Observaciones***
I	Organizar y distribuir del trabajo.	Lorena Naranjo	x												
I	Diseñar la metodología del procesamiento	Lorena Naranjo	x												
	Obtener de información	Lorena Naranjo / estudiantes DER 903-2	x	x											
	Organizar resoluciones.	Lorena Naranjo / estudiantes DER 903-2	x	x											
	Sistematizar resoluciones.	Lorena Naranjo / estudiantes DER 903-2	x	x											
	Presentar y revisar informe parcial	Lorena Naranjo / tesista y estudiantes DER 903-2			x										
	Elaborar fichas de resumen.	Estudiantes DER 903-2			x	x									
	Presentar y revisar informe parcial	Lorena Naranjo / tesista y estudiantes DER 903-2					x	x							
	Crear TESAURO	Estudiantes DER 903-2			x	x									

	Presentar y revisar informe parcial	Lorena Naranjo / tesista y estudiantes DER 903-2					x	x							
	Elaborar informe final	Lorena Naranjo / tesista y estudiantes DER 903-2							x	x					
	Revisar informe	Lorena Naranjo y tesista									x	x			
	Incluir resultados de la investigación en tesis doctoral	Lorena Naranjo											x	x	

REFERENCIAS BIBLIOGRÁFICAS

A. Millar, "The Assault on Privacy", The University of Michigan Press, Ann Arbor, 1971, pp. 185 ss, fecha de consulta 16 de junio del 2007 en

http://portal.acm.org/citation.cfm?id=1017625.1017632&coll=GUIDE&dl=GUIDE&CFID=442837&CFTOKEN=90223178

Antonio Enrique Pérez Luño, Manual de Informática, Ariel. Barcelona, 1.996, p.1.

Carlos Ruiz Miguel, El derechos a la protección de la vida privada en la Jurisprudencia del Tribunal Europeo de Derechos Humanos, Cuaderno Civitas, Madrid, 1994, p. 50

Convenio 108/81 CE del Consejo, de 28 de enero, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Francisco Sardina Ventosa, El derecho a la intimidad informática y el tratamiento de datos personales para la prevención del fraude, Actualidad Informática Aranzadi: revista informática para juristas. 1997. Fecha de consulta, 15 de junio del 2007 en http://intra.pre.gva.es/convera/docpdf_castellano/articulosrevista/13a16/sardinaventosa97.pdf

Herminia Campuzano Tomé, Vida Privada y datos personales, Editorial Tecnos, Madrid, 2000, p. 66

María Mercedes Serrano Pérez; El derecho fundamental a la protección de datos, Derecho español y comparado, Thomson Civitas, 1era ed., Madrid, 2002, p. 29.

Oswaldo Gozaini, Hábeas Data, protección de datos personales, Rubinzal- Culzoni Editores, Buenos Aires, 2001, p. 9.

Pablo A. Palazzi, La Transmisión Internacional de Datos Personales y la Protección de la Privacidad Argentina, América Latina, Estados Unidos y la Unión Europea, Buenos Aires, Ad Hoc, pp. 99 y ss.

Pablo Lucas Murillo de la Cueva; Diez preguntas sobre el derecho a la autodeterminación informativa y la protección de datos de carácter personal, Agencia Catalana de Protección de Datos publicado el 13/01/2006. Fecha de consulta, 6 de junio del 2007 en la página http://www.apd.cat/es/llistaArticles.php?cat_id=175&pageID=4

Pablo Lucas Murillo, El derecho a la autodeterminación informativa, editorial Tecnos, Madrid, 1990, p.131.

Recomendación del Consejo, de 1 de octubre de 1980, relativa a los Flujos Transfronterizos para el Desarrollo Económico y Social.

Resolución 68/509/CE, sobre los derechos humanos y los nuevo logros científicos, Sentencia de 15 de diciembre de 1983, BJC núm. 33, IV Jurisprudencia Constitucional Extrajera, 1984.

Sentencia de 15 de diciembre de 1983, BJC núm. 33, IV Jurisprudencia Constitucional Extrajera, 1984.

STC 254/1993, de 20 de julio. España.

Tratado por el que se establece una Constitución para Europa, edición preparada por: Francisco Aldecoa Luzárraga, 2da ed. Madrid, 2004 fecha de consulta 16 de junio del 2007 en http:// www.realinstitutoelcano.org/especiales/constitucioneuropea/nuevo/

Tratado por el que se establece una Constitución para Europa, edición preparada por: Francisco Aldecoa Ximena Puente de la Mora, Latinoamérica ante la tendencia europea y norteamericana en la regulación del flujo transfronterizo de datos personales, fecha de consulta 16 de junio del 2007 en http://www.alfa-redi.org/rdi-articulo.shtml?x=7858

2. MATRIZ DE PROCESAMIENTO:

MATRIZ DE PROCESAMIENTO

Estimados estudiantes se encuentra listo el formulario pueden empezar el procesamiento de jurisprudencia para su segundo progreso.

Si tienes problemas para visualizar o enviar este formulario, puedes rellenarlo online:
https://docs.google.com/forms/d/1fWvWJdrHr6ihmoDdlhIuChaXdzjEjG8TWqPswmKoEmc/viewform?c=0&w=1&usp=mail_form_link

Jurisprudencia sobre derecho a la protección de datos yhábeas data

Análisis jurisprudencial sobre derecho a la protección de datos y hábeas data desde 1993 hasta 2014

*Obligatorio

Año de investigación *

No. de expediente de Corte Constitucional *

Por favor incluir todos los datos que consten en el proceso números, letras y año.

Juzgado de procedencia *

Ejemplo: Juzgado Primero de lo Civil de Guayaquil

Tipo de acción *

Por ejemplo: Acción de hábeas data

Pronunciamiento: Juez Primer Nivel *

- Acepta
- Rechaza

Pronunciamiento: Juez de Apelación

- Rechaza el recurso y confirma

- ○ Acepta el recurso y revoca la sentencia de primera instancia
- ○ Acepta
- ○ Revoca la resolución del Juez de Primera instancia y acepta parcialmente la demanda

X

- ○ Otro:

Institución que emite el fallo constitucional:

- ○ Sala de lo Constitucional de la Corte Suprema de Justicia
- ○ Tribunal Constitucional
- ○ Corte Constitucional de Transición (2008-2012)
- ○ Corte Constitucional

Parámetros de sentencia. Legitimado Activo: *

Actor de la acción presentada

- ○ masculino
- ○ femenino
- ○ LGTBI
- ○ persona jurídica
- ○ organización social
- ○ colectivo
- ○ individual
- ○ público
- ○ privado

Parámetros de sentencia. Legitimado pasivo: *

Demandado de la acción presentada

- ○ masculino
- ○ femenino
- ○ LGTBI
- ○ persona jurídica
- ○ organización social
- ○ colectivo
- ○ individual
- ○ público
- ○ privado

Decisión de la resolución constitucional: *

- ○ Acepta
- ○ Niega
- ○ Niega, incumplimiento de requisitos
- ○ Deja sin efecto

Fecha de expedición de la resolución constitucional *

2014

Establezca el Registro Oficial donde ha sido publicada la resolución constitucional:

Por favor! utilizar la fórmula de R. O. Suplemento 572, 10 noviembre 2011

TESAURO *

Es una herramienta de control terminológico, llamado también sistema de vocabulario controlado y dinámico o sistema de indización controlado, que establece relaciones entre los distintos términos contenidos en él y se aplica a un campo específico del conocimiento. Ejemplo: Hábeas Data / acceso a base de datos / datos bancarios / injurias

Vulneración de derecho alegada *

Otro

- derecho a la protección de datos personales
- acceso a bases de datos personales
- datos personales
- hábeas data
- procedimiento de hábeas data
- intimidad
- bueno nombre
- identidad
- privacidad
- derecho a la propia imagen
- Otro:

Análisis constitucional: I. Hechos relevantes: *

A manera de ejemplo: a) La legitimada activa manifestó que es titular de una cuenta en el Banco del Pichincha, no obstante, señaló que al acercarse a realizar un retiro de su cuenta le informaron que se encontraba inactiva, por lo que acudió a la agencia del banco en Riobamba donde le comunicaron que le había clausurado su cuenta bancaria porque ella tenía vinculación el lavado de dinero. b) Indicó que solicitó por escrito una explicación de lo suscitado a la entidad financiera y pidió se le entreguen copias certificadas de todo el trámite que sirvió de base para que se le cancelara su cuenta, sin embargo, dijo que no ha tenido respuesta alguna. c) Por lo expuesto, la accionante presentó una acción dehábeas data en contra del Banco Pichincha para que se le suministre información que detalle los motivos por los cuales cerraron su cuenta bancaria. d) Los representantes de la entidad bancaria dieron a conocer que jamás se ha vertido versión que refiera que el cierre de la cuenta de la accionante es por tener relación con el lavado de dinero, sino que se procedió de esa manera en aplicación de lo establecido en la cláusula octava del contrato de cuenta de ahorros.

Análisis constitucional: II. Revisar los considerandos sobre la valoración de los derechos y los de resolución. En el caso de la Corte Constitucional, revisar: Problemas jurídicos identificados por la Corte Constitucional *

A manera de ejemplo: 1. ¿En qué difiere la acción de hábeas data del proceso ordinario de exhibición de documentos? 2. ¿En qué medida pueden considerarse personales los datos constates en los registros de instituciones bancarias?

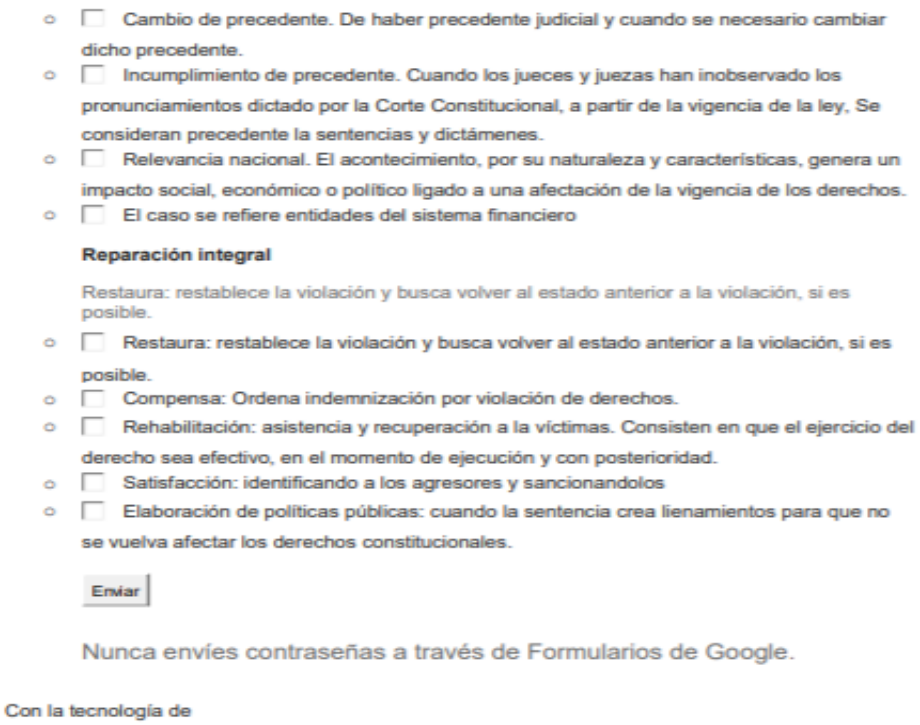
Análisis constitucional: III. Descripción breve de la sentencia emitida por el/los jueces que conocieron la causa.*

A manera de ejemplo: El Juzgado Cuarto de lo Civil, Mercantil e Inquilinato de Carchi rechazó la acción planteada. El despacho manifestó que hábeas data confiere al accionante el derecho a solicitar al funcionario correspondiente, la actualización, rectificación, eliminación o anulación de datos si fueren erróneos o cuando afectaren sus derechos, pero no puede servir la presente acción como diligencia preparatoria para la iniciación de un proceso judicial diferente. Concluyó que lo pretendido por la accionante es que se exhiban documentos que reposan en los archivos del Banco Pichincha, entidad a la que verdaderamente pertenecen los documentos y no a la accionante.

Análisis constitucional: IV. Argumentos sobre la relevancia constitucional

Gravedad. Se tendrá en cuenta la gravedad del caso (vulneración del derecho frente a la dignidad de la persona) y que las vías judiciales ordinarias no sean idóneas para la reparación del derecho.

- ☐ Gravedad. Se tendrá en cuenta la gravedad del caso (vulneración del derecho frente a la dignidad de la persona) y que las vías judiciales ordinarias no sean idóneas para la reparación del derecho.
- ☐ Novedad del Caso. Que sea un caso inédito en relación con los derechos y garantías establecidos en la Constitución.
- ☐ Falta de precedente judicial. Que la Corte Constitucional no haya emitido pronunciamientos referentes al problema jurídico general en caso similares.


- ☐ Cambio de precedente. De haber precedente judicial y cuando se necesario cambiar dicho precedente.
- ☐ Incumplimiento de precedente. Cuando los jueces y juezas han inobservado los pronunciamientos dictado por la Corte Constitucional, a partir de la vigencia de la ley, Se consideran precedente la sentencias y dictámenes.
- ☐ Relevancia nacional. El acontecimiento, por su naturaleza y características, genera un impacto social, económico o político ligado a una afectación de la vigencia de los derechos.
- ☐ El caso se refiere entidades del sistema financiero

Reparación integral

Restaura: restablece la violación y busca volver al estado anterior a la violación, si es posible.

- ☐ Restaura: restablece la violación y busca volver al estado anterior a la violación, si es posible.
- ☐ Compensa: Ordena indemnización por violación de derechos.
- ☐ Rehabilitación: asistencia y recuperación a la víctimas. Consisten en que el ejercicio del derecho sea efectivo, en el momento de ejecución y con posterioridad.
- ☐ Satisfacción: identificando a los agresores y sancionandolos
- ☐ Elaboración de políticas públicas: cuando la sentencia crea lienamientos para que no se vuelva afectar los derechos constitucionales.

Enviar

Nunca envíes contraseñas a través de Formularios de Google.

Con la tecnología de

3. RESULTADOS DE LA INVESTIGACIÓN

Adjunto archivo en Excel.

ANEXO 2

1. **AÑO: 2018**

1.1 PRENSA ESCRITA

1.1.1 Nacional

1. A proteger los datos públicos (15 de febrero de 2018), *La Hora*, pág. B4 sección País. Recuperado de link
2. Los datos personales no tienen protección (29 de abril de 2018), *el Universo, Portada.* Recuperado del link
3. Ecuador no tiene ley para proteger datos personales (29 de abril de 2018), *El Universo,* pág. A8 y A9. Recuperado de link
4. Lorena Naranjo: Protección de la información es un derecho, (29 de abril de 2018), *El Universo, edición impresa*, pág. A9. Recuperado de link
5. Naranjo Cruz, Eduardo, (22 de junio de 2018), Protección de datos, *La Hora*, pág. A4. Recuperado de link
6. (15 de noviembre de 2018), Lorena Naranjo: 'Cómo obtuvieron datos para la llamada, ahí ley entra en acción', El Universo, pág. A4. Recuperado de link
7. Editorial, (19 de noviembre de 2018), Protección de Datos, El Universo. Recuperado de link

1.1.2 Provincias

1. (26 de noviembre de 2018), Samantha Manzano Ruales, nueva Ley Orgánica de Datos Personales, El Norte (Ibarra). Recuperado de link
2. (23 de noviembre de 2018), Llaman para debatir ley de datos personales, El Mercurio – Cuenca, pág. 7A Recuperado de link
3. (23 de noviembre de 2019), Proponen regular difusión de los datos personales, El Mercurio – Cuenca. Recuperado de link
4. (21 de noviembre de 2018), Llaman para debatir ley de datos personales, *El Mercurio – Cuenca*, link
5. (17 de noviembre de 2018), Mesas de diálogo para Ley de Protección de Datos, El Heraldo – Cañar. Recuperado de link

1.2 PERIÓDICO ONLINE

1. (06 de marzo de 2018), Dinardap recoge criterios de entidades del sector de Telecomunicaciones para el proyecto de Ley de Protección de Datos Personales, *Informateypunto (diario digital),* Tecnología. Recuperado de link
2. (15 de marzo de 2018), Mintel y Dinardap trabajan en una estrategia para la protección de los datos personales, *Informateypunto (diario digital),* Tecnología. Recuperado de link
3. (29 de abril de 2018), Ecuador no tiene ley para proteger datos personales, *El Universo, edición digital*. Recuperado de link

4. Lorena Naranjo: Protección de la información es un derecho, (29 de abril de 2018), *El Universo*, edición digital. Recuperado de link
5. (18 de mayo de 2018), "La Protección de datos es un derecho constitucional": Lorena Naranjo Godoy, *Infórmate y Punto (Diario digital),* Tecnología. Recuperado de link
6. (24 de mayo de 2018), La Dinardap destaca la Protección de Datos, en Congreso de Ciberseguridad de Banca y Gobierno, *Infórmate y Punto (diario digital),* Tecnología. Recuperado de link
7. (11 de junio de 2018), Falta de Ley de Protección de Datos Públicos traba entendimiento entre Ecuador y México, *Ecuador Inmediato (diario digital).* Recuperado de link
8. (12 de junio de 2018), Ecuador no tiene una ley de protección de datos personales, *Diario Expreso* . Recuperado de link
9. (18 de junio de 2018), Alistan anteproyecto de ley para proteger datos personales de los ecuatorianos, *Agencia Andes, diario digital suprimido*. Recuperado de link
10. Naranjo Cruz, Eduardo, (22 de junio de 2018), Protección de datos, *La Hora.* Recuperado de link
11. (10 de julio de 2018, Ecuador presentó políticas públicas para la era digital, El Telégrafo. Recuperado de link
12. (02 de julio de 2018), Ecuador necesita una Ley de Protección de Datos Personales con visión técnica, *Infórmate y punto*. Recuperado de link
13. (25 de septiembre de 2018), Impacto e importancia de la Ley de Protección de Datos Personales para Ecuador fue analizado en la Universidad Andina, *Infórmate y punto.* Recuperado de link
14. (22 de octubre de 2018), Es ilegal usar los datos personales sin autorización, *El Universo*. Recuperado de link
15. (28 de octubre de 2018), Protección de datos, *El Universo - Cartas al director*. Recuperado de link
16. (14 de noviembre de 2018) Lorena Naranjo: 'Cómo obtuvieron datos para la llamada, ahí ley entra en acción', El Universo. Recuperado de link
17. Editorial, (19 de noviembre de 2019), Protección de Datos, El Universo, pág. A5. Recuperado de link
18. (23 de noviembre de 2018), Dinardap propone regular difusión de datos personales, Ecuadorinmediato.com. Recuperado de link
19. (11 de diciembre de 2018), El Observatorio de Información de Datos en Latinoamérica lanza una campaña por la protección de datos en Ecuador, Portal apc.org. Recuperado de link

1.3 RADIO

1. Vilatuña, Martha, (21 de septiembre de 2018), Ley de Protección de Datos Personales Radio Vigía Al Día (entrevista). Recuperado de link

1.4 TELEVISIÓN

1. (27 de noviembre de 2018), Anteproyecto de Ley de Protección de Datos Personales, ENTV (Ibarra). Recuperado de link

1.5 BOLETINES

1. Dirección de Comunicación Social. (10 de abril de 2018). Representante de la Sociedad Civil conoce detalles sobre el anteproyecto de la Ley de Protección de Datos. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/representante-de-la-sociedad-civil-conoce-detalles-sobre-el-anteproyecto-de-la-ley-de-proteccion-de-datos/

2. Dirección de Comunicación Social. (10 de abril de 2018). Representante de la Sociedad Civil conoce detalles sobre el anteproyecto de la Ley de Protección de Datos. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/representante-de-la-sociedad-civil-conoce-detalles-sobre-el-anteproyecto-de-la-ley-de-proteccion-de-datos/

3. Dirección de Comunicación Social. (10 de abril de 2018). Representante de la Sociedad Civil conoce detalles sobre el anteproyecto de la Ley de Protección de Datos. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/representante-de-la-sociedad-civil-conoce-detalles-sobre-el-anteproyecto-de-la-ley-de-proteccion-de-datos-2/

4. Dirección de Comunicación Social. (11 de abril de 2018). Anteproyecto de la Ley de Protección de Datos será el tema central en conversatorio en la Universidad Andina. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/anteproyecto-de-la-ley-de-proteccion-de-datos-sera-tema-central-en-conversatorio-en-la-universidad-andina/

5. Dirección de Comunicación Social. (16 de julio de 2018). Anteproyecto de la Ley de Protección de Datos será el tema central en conversatorio en la Universidad Andina.. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/anteproyecto-de-la-ley-de-proteccion-de-datos-sera-el-tema-central-en-conversatorio-en-la-universidad-andina/

6. Dirección de Comunicación Social. (10 de julio de 2018). Estudiantes universitarios reciben reconocimiento por aporte al anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/estudiantes-universitarios-reciben-reconocimiento-por-aporte-al-anteproyecto-de-ley-de-proteccion-de-datos-personales/

7. Dirección de Comunicación Social. (12 de julio de 2018). Estudiantes de Derecho aportan con sus conocimientos en el anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/estudiantes-de-derecho-aportan-con-sus-conocimientos-en-el-anteproyecto-de-ley-de-proteccion-de-datos-personales/

8. Dirección de Comunicación Social. (20 de julio de 2018). Especialistas en protección de datos se darán cita para analizar el anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/expertos-en-proteccion-de-datos-analizaran-el-anteproyecto-de-ley-de-proteccion-de-datos-personales/

9. Dirección de Comunicación Social. (31 de julio de 2018). Especialistas debatieron sobre la incorporación de la Seguridad Informática en el anteproyecto de Ley de Protección de Datos. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/especialistas-debatieron-sobre-la-incorporacion-de-la-seguridad-informatica-en-el-anteproyecto-de-ley-de-proteccion-de-datos/

10. Dirección de Comunicación Social. (07 de agosto de 2018). Principios y derechos fueron tratados durante la segunda ronda para la construcción del anteproyecto de Ley de Protección de Datos. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/principios-y-derechos-fueron-tratados-durante-la-segunda-ronda-para-la-construccion-del-anteproyecto-de-ley-de-proteccion-de-datos/

11. Dirección de Comunicación Social. (07 de agosto de 2018). El anteproyecto de Ley de Protección de Datos se analizará en el Encuentro que organiza la Asociación Ecuatoriana de Software. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/el-anteproyecto-de-ley-de-proteccion-de-datos-se-analizara-en-el-encuentro-que-organiza-la-asociacion-ecuatoriana-de-software/

12. Dirección de Comunicación Social. (24 de agosto de 2018). La Dinardap analizará conjuntamente con la sociedad civil el contenido del anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/6604-2/

13. Dirección de Comunicación Social. (31 de octubre de 2018). En noviembre, Dinardap retoma las mesas de diálogo para tratar el anteproyecto de Ley de Protección de Datos. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/en-noviembre-dinardap-retoma-las-mesas-de-dialogo-para-tratar-el-anteproyecto-de-ley-de-proteccion-de-datos/

14. Dirección de Comunicación Social. (06 noviembre de 2018). Construcción del anteproyecto de Ley de Protección de Datos Personales continúa en noviembre. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/construccion-del-anteproyecto-de-ley-de-proteccion-de-datos-personales-continua-en-noviembre/

15. Dirección de Comunicación Social. (14 noviembre de 2018). Anteproyecto de Ley de Protección de Datos se expuso a empresarios en sesión Webinar. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/anteproyecto-de-ley-de-proteccion-de-datos-se-expuso-a-empresarios-en-sesion-webinar/

16. Dirección de Comunicación Social. (16 noviembre de 2018). Hasta diciembre del 2018 se prevé contar con un Anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/hasta-diciembre-del-2018-se-preve-contar-con-un-anteproyecto-de-ley-de-proteccion-de-datos-personales/

17. Dirección de Comunicación Social. (19 noviembre de 2018). Universidad Técnica de Ambato será sede de las mesas de diálogo del Anteproyecto de Ley de Protección de Datos. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/universidad-tecnica-de-ambato-sera-sede-de-las-mesas-de-dialogo-del-anteproyecto-de-ley-de-proteccion-de-datos/

18. Dirección de Comunicación Social. (19 noviembre de 2018). Avanzan mesas de diálogo para la construcción participativa del Anteproyecto de Ley de Protección de Datos. Sitio institucional DINARDAP. Recuperado de

http://www.datospublicos.gob.ec/avanzan-mesas-de-dialogo-para-la-construccion-participativa-del-anteproyecto-de-ley-de-proteccion-de-datos/

19. Dirección de Comunicación Social. (19 noviembre de 2018). Mesas de diálogo para la construcción participativa del Anteproyecto de Ley de Protección de Datos se realizarán en Ibarra. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/mesas-de-dialogo-para-la-construccion-participativa-del-anteproyecto-de-ley-de-proteccion-de-datos-se-realizaran-en-ibarra/

20. Dirección de Comunicación Social. (19 noviembre de 2018). Inicia la segunda fase de las mesas de diálogo para la construcción participativa del Anteproyecto de Ley de Protección de Datos. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/inicia-la-segunda-fase-de-las-mesas-de-dialogo-para-la-construccion-participativa-del-anteproyecto-de-ley-de-proteccion-de-datos/

21. Dirección de Comunicación Social. (21 noviembre de 2018). Dinardap recibe propuestas de Amcham sobre anteproyecto de ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/dinardap-recibe-propuestas-de-amcham-sobre-anteproyecto-de-ley-de-proteccion-de-datos-personales/

22. Dirección de Comunicación Social. (22 noviembre de 2018). Primer día de mesas de diálogo para construcción del Anteproyecto de Ley de Protección de Datos se realizó en Cuenca. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/primer-dia-de-mesas-de-dialogo-para-construccion-del-anteproyecto-de-ley-de-proteccion-de-datos-se-realizo-en-cuenca/

23. Dirección de Comunicación Social. (27 noviembre de 2018). Medios de comunicación de Ibarra mostraron su interés en el anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/medios-de-comunicacion-de-ibarra-mostraron-su-interes-en-el-anteproyecto-de-ley-de-proteccion-de-datos-personales/

24. Dirección de Comunicación Social. (27 noviembre de 2018). Estudiantes y académicos interesados en conocer sobre el anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de

http://www.datospublicos.gob.ec/estudiantes-y-academicos-interesados-en-conocer-sobre-el-anteproyecto-de-ley-de-proteccion-de-datos-personales/

25. Dirección de Comunicación Social. (27 noviembre de 2018). En Ibarra, la Dinardap desarrolló las mesas de diálogo para la construcción del anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/en-ibarra-la-dinardap-desarrollo-las-mesas-de-dialogo-para-la-construccion-del-anteproyecto-de-ley-de-proteccion-de-datos-personales/

26. Dirección de Comunicación Social. (29 de noviembre de 2018). Continúan las jornadas para la construcción del Anteproyecto de Ley de Protección de Datos Personales en Manta. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/segunda-fase-de-las-mesas-de-dialogo-para-la-construccion-del-anteproyecto-de-ley-de-proteccion-de-datos-personales-finaliza-en-manta/

27. Dirección de Comunicación Social. (3 diciembre, 2018). Representantes de la Función Legislativa conocieron sobre el Anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/representantes-de-la-funcion-legislativa-conocieron-sobre-el-anteproyecto-de-ley-de-proteccion-de-datos-personales/

28. Dirección de Comunicación Social. (06 de diciembre de 2018 – 13:00). Ambato fue la sede del cuarto día de las mesas de diálogo del anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de http://www.datospublicos.gob.ec/ambato-fue-la-sede-del-cuarto-dia-de-las-mesas-de-dialogo-del-anteproyecto-de-ley-de-proteccion-de-datos-personales/

2. AÑO: 2019

2.1 PRENSA ESCRITA

2.1.1 Nacional

1. Cazar, Diego, columnista, (10 de mayo de 2019), Se nos va el tren digital, *Diario La Hora Opinión*. Recuperado de link

2. Se busca protección sobre datos de carácter personal, (16 de enero de 2019), *Diario La Hora, pág. A7* – Nacional. Recuperado de link
3. Naranjo Cruz, Eduardo, columnista, (17 de mayo de 2019), Seguridad digital, *Diario La Hora Opinión*. Recuperado de link
4. Orozco, Mónica, columnista, (24 de junio de 2019), Acoso telefónico, El Comercio, Economía a pie. Recuperado de link
5. Naranjo Cruz, Eduardo, columnista, (25 de enero de 2019), Información segura, *Diario La Hora, Opinión, pág.A4.* Recuperado de link
6. Los datos personales fluyen sin control (06 de julio de 2019), *El Comercio, Portada*. Recuperado de link
7. González, Patricia, Los datos personales pasan de mano en mano, sin control, (06 de julio de 2019), *El Comercio, pág. A2-Actualidad*. Recuperado de link
8. Maldonado, Carla, entrevistadora (21 de julio de 2019), El personaje de la semana: Los datos personales son el nuevo petróleo de las empresas, *El Telégrafo - A7* – Recuperado de link
9. Cazar Baquero, Diego, columnista (30 de agosto de 2019), Ecuador digital, *Diario La Hora, Opinión*. Recuperado de link
10. (30 de septiembre de 2019), En Ecuador: ¿Sus datos ya no le pertenecen?, *revista Vistazo, Portada*. Recuperado de link
11. Editorial, (30 de septiembre de 2019), Minería de datos, revista Vistazo. Recuperado de link
12. (30 de septiembre de 2019), Nada es privado. Revista Vistazo, pág. 42,44 y 45. Recuperado de link
13. Medina Luis, (30 de septiembre de 2019), Seguridad no tan segura, pág. 92-93, revista Vistazo. Recuperado de link
14. Inicia investigación legislativa por filtración de datos, (02 de octubre de 2019), Expreso. Recuperado de link
15. (01 de octubre de 2019), Tres temas generan debate en la Ley de Datos, El Comercio, Economía, página A6. Recuperado de link

2.1.2 Provincias

1. (15 de enero de 2019), El objetivo (de la ley) es proteger los datos personales, El Mercurio (Cuenca). Recuperado del link
2. (02 de agosto de 2019), Mesas buscan potenciar el comercio electrónico. El Tiempo (Cuenca) Recuperado de link

2.1.3 PERIÓDICO ONLINE

1. ¿Qué propone la Ley Orgánica de Protección de Datos Personales en Ecuador?, (21 de enero de 2019), Revista Gestión. Recuperado de link

2. Se busca protección sobre datos de carácter personal, (16 de enero de 2019), La Hora. Recuperado de link
3. Naranjo Cruz, Eduardo, columnista, (25 de enero de 2019), Información segura, *Diario La Hora, Opinión, pág.A4.* Recuperado de link
4. Naranjo Cruz, Eduardo, columnista, (17 de mayo de 2019), Seguridad digital, *Diario La Hora Opinión.* Recuperado de link
5. Cazar, Diego, (10 de mayo de 2019), Se nos va el tren digital, *La Hora Opinión*. Recuperado de link
6. Ecuador es uno de los tres países de la región donde falta una ley que proteja los datos personales, (10 de junio de 2019), *Diario Primicias, Negocios*. Recuperado de link
7. Orozco, Mónica, columnista, (24 de junio de 2019), Acoso telefónico, *El Comercio, Economía a pie.* Recuperado de link
8. Lorena Naranjo: 'Los 'call center' saben mucho de nosotros, pero no hay una Ley que vele para que esos datos se usen de forma responsable', (27 de junio de 2019), *El Comercio, Negocios.* Recuperado de link
9. González, Patricia, Los datos personales pasan de mano en mano, sin control, (06 de julio de 2019), *El Comercio*. Recuperado de link
10. Maldonado, Carla, entrevistadora (21 de julio de 2019), "Los datos personales son el nuevo petróleo para las empresas", El Telégrafo, Política. Recuperado de link
11. El proyecto de Ley de Datos Personales fue entregado a la Asamblea, (19 de septiembre de 2019), *El Telégrafo, Política.* Recuperado de link
12. Uso de información personal está penado con prisión, (20 de septiembre de 2019), *La Hora, País.* Recuperado de link
13. Empresa Eliminalia se ofrece a borrar datos filtrados de ecuatorianos, (20 de septiembre de 2019), *El Telégrafo, Política*. Recuperado de link
14. Los datos personales podrán usarse solo temporalmente, (20 de septiembre de 2019), *El Telégrafo, Política*. Recuperado de link
15. Cazar Baquero, Diego, columnista (30 de agosto de 2019), Ecuador digital, *Diario La Hora, Opinión*. Recuperado de link
16. (17 de septiembre de 2019), El Gobierno ecuatoriano impulsa proyecto de protección de datos tras filtración masiva, *Agencia Internacional Sputnik*. Recuperado de link
17. Orozco, Mónica, (17 de septiembre de 2019), En Ecuador debemos tener una conciencia de protección de datos. *El Comercio*. Recuperado de link
18. Rueda, Carlos Roberto, (17 de septiembre de 2019), Una ley para contener puntos de fuga de datos, Expreso. Recuperado de link
19. (17 de septiembre de 2019), Filtración de datos: "Gobierno conocía de esta divulgación desde el 11 de septiembre", Metro Hoy. Recuperado de link
20. Dávalos, Nelson, entrevistador, (19 de septiembre de 2019), El 'derecho al olvido' llegará a Ecuador con la nueva ley de datos, *diario digital Primicias*. Recuperado de link
21. Proyecto de ley de protección de datos en Ecuador es presentado por Mintel, (19 de septiembre), *El Comercio, Actualidad*. Recuperado de link
22. Proyecto de ley propone multa del 17% de la facturación a empresas por mal uso de datos, (19 de septiembre de 2019), *El Comercio, Actualidad*. Recuperado de link

23. Rueda, Carlos Roberto, La Ley de Protección de Datos está en manos de la Asamblea Nacional, (19 de septiembre de 2019), *Expreso*. Recuperado de link
24. (19 de septiembre de 2019), En Ecuador existe un mercado negro de venta de datos, reconoce ministro de Telecomunicaciones, *diario digital Primicias*. Recuperado de link
25. Dos años 'de gracia' para adaptarse a la Ley de Protección de Datos, (20 de septiembre de 2019), *El Universo, Política*. Recuperado de link
26. Ley propone incluir en la malla curricular la educación digital, (20 de septiembre de 2019), *El Comercio, Actualidad.* Recuperado de link
27. Rueda, Carlos Roberto, El control del uso de datos se ata al Gobierno, (20 de septiembre de 2019), *Expreso, Actualidad.* Recuperado de link
28. Rueda, Carlos Roberto, entrevistador, (26 de septiembre de 2019), Lorena Naranjo: "La modernidad está aquí y no fuimos al mismo ritmo legal", *Expreso, Seguridad Informática*. Recuperado de link
29. (26 de septiembre de 2019), Minería de Datos, *revista Vistazo, editorial*. Recuperado de link
30. Pérez, Alejandro (27 de septiembre de 2019), Nada es privado, revista Vistazo. Recuperado de link, link, link
31. (27 de septiembre de 2019), Ecuador necesita urgente una Ley de Protección de Datos Personales. Recuperado de link
32. Vélez, Roger, (02 de octubre de 2019), Comisión de Soberanía inició investigación sobre filtración de datos y tramitará proyecto de ley, El Comercio, Política. Recuperado de link
33. (03 de octubre de 2019), Ecuador: sin responsables claros sobre filtración de datos, Diario La Hora, País. Recuperado de link

2.1.4 RADIO

1. Naranjo, Susana, entrevistador, (07 de enero de 2019) Ley de Protección de Datos Personales *Radio Católica*, 06:15. Recuperado de link
2. Vilatuña, Martha, entrevistadora, (09 de enero de 2019), Ley de Protección de Datos Personales, *Radio Vigía*, 06:15. Recuperado de link
3. Andrés Carrión, entrevistador (14 de enero de 2019), Ley de Protección de Datos Personales, *Radio Platinium*, 17:00. Recuperado de link
4. Vilatuña, Martha, entrevistadora, (29 de abril de 2019), Ley de protección de datos personales, *Radio Vigía, Al Día,* 06.15. Recuperado de link
5. Cajo, Fernando Entrevistador, (30 de abril de 2019), Imperiosa necesidad de tener una Ley de protección de datos personales, *Radio Distrito, De Vuelta*, 17:00. Recuperado de link
6. Montero, Nancy (01 de agosto de 2019) - Entrevista Dra. Lorena Naranjo, sobre el proyecto de Ley de Protección de Datos Personales, *radio Pública*. Recuperado de link

7. Rivadeneira, Miguel, entrevistador (18 de septiembre de 2019), La educación digital es parte del Proyecto de Ley de Protección de Datos Personales, radio Quito, retransmitido por Televicentro. Recuperado de link
8. Montalvo, Daniel, entrevistador (18 de septiembre de 2019), Ley de Protección de Datos Personales, Radio Centro. Recuperado de link
9. Pérez, Milton, (19 de septiembre de 2019) La Ley de Protección de Datos Personales le da al ciudadano poder sobre su información, *radio Sucesos*, Recuperado de link
10. (19 de septiembre de 2019), Ley de Protección de Datos Personales, *radio Platinium-Servicio informativo.* Recuperado de link
11. Ñacato, Jorge, entrevistador, (20 de septiembre de 2019), El derecho a la protección de datos personales nace con la era digital, *radio América, Buenos días América.* Recuperado de link
12. Vilatuña, Martha, entrevistadora, (23 de septiembre de 2019), Los ciudadanos deben saber cuáles son sus derechos digitales, r*adio Vigía, Al día*, Recuperado de link
13. Moposita Garcés, Wilson y Espinel, Lisenia, entrevistadores, (23 de septiembre de 2019), La Ley de Protección de Datos Personales no solo involucra la seguridad, *Radio Sonorama, La Palabra*. Recuperado de link
14. Vázquez, Edgar, entrevistador, (27 de septiembre de 2019), Solo empoderando a los ciudadanos de sus derechos se protegen sus datos, *radio Rumba*. Recuperado de link
15. Vela, Fabricio y Moncayo, Alexis, entrevistadores, (01 de octubre de 2019), Diversos sectores participaron en la construcción del proyecto de Ley de Datos Personales, r*adio Majestad, A primera hora*. Recuperado de link
16. Cajo, Fernando, entrevistador, (02 de octubre de 2019), Los derechos digitales se deben nutrir con la educación digital, *radio CRE Satelital de Guayaquil*. Recuperado de link
17. (02 de octubre de 2019), El proyecto Ley de Protección de Datos Personales menciona a una autoridad de protección, *radio La Única*. Recuperado de link
18. Rivadeneira, Miguel, entrevistador (12 de octubre de 2019), El proyecto Ley de Protección de Datos Personales, *radio Quito, programa Controversia*. Recuperado del link
19. Rivadeneira, Miguel, entrevistador (13 de octubre de 2019), El proyecto Ley de Protección de Datos Personales, *radio Platinium, programa Controversia*. Recuperado del link

2.1.5 TELEVISIÓN

1. Murillo, Ramón, entrevistador, (28 de julio de 2019), Especial Big data, Ecuavisa - Visión 360. Recuperado de link
2. Murillo, Ramón, entrevistador, (28 de julio de 2019), *Ecuavisa - Visión 360, Especial Big data*. Recuperado de link

3. Del Pozo, Eduardo entrevistador, (24 de agosto de 2019), Entrevista a Lorena Naranjo Godoy - Protección de Datos, *Telesucesos canal 29, Programa Quiteños*. Recuperado de link
4. (13 de septiembre de 2019), Sanciones contempladas en la Ley de Protección de Datos Personales, *Ecuavisa, Televistazo al mediodía*, Recuperado de link
5. (16 de septiembre de 2019), La Ley de Protección de Datos Personales le da al ciudadano poder sobre su información, *Ecuavisa noticiero al mediodía*. Recuperado de link
6. Cañizares, Ana María, (16 de septiembre de 2019), Gobierno de Ecuador investiga supuesta filtración masiva de datos de casi todos sus ciudadanos, CNN en Español. Recuperado de link
7. Rivadeneira, Miguel, entrevistador (18 de septiembre de 2019), La educación digital es parte del Proyecto de Ley de Protección de Datos Personales, *radio Quito, retransmitido por Televicentro*. Recuperado de link
8. Hinostroza, Janeth, entrevistadora, (19 de septiembre de 2019), Normativa de protección informática de datos, *Teleamazonas, Los Desayunos de 24horas*. Recuperado de link
9. (19 de septiembre de 2019), Proyecto de Ley de Protección de Datos Personales incluye sanciones, *Ecuavisa, Televistazo, noticiero estelar*. Recuperado de link
10. (19 de septiembre de 2019), La Ley de Protección de Datos Personales regularía el uso de bases de datos, *Telediario (TVC) noticiero estelar (20:30)*. Recuperado de link
11. Hidalgo, Christian, entrevistador, (19 de septiembre de 2019), Mayor control a empresas dedicadas a la administración de datos, *TCTelevisión noticiero mediodía*, Recuperado de link
12. (19 de septiembre de 2019), Ley de protección de datos personales, *Tc Televisión, noticiero estelar(19:05).* Recuperado de link
13. (19 de septiembre de 2019), Ley de protección de datos personales, *Teleamazonas, noticiero estelar (20:08).* Recuperado de link
14. (19 de septiembre), Entrega de Ley de protección de datos personales, *Canal Uno, noticiero estelar (20:05).* Recuperado de link
15. (19 de septiembre de 2019), Ley de Protección de Datos Personales, *Telerama, noticiero estelar*. Recuperado de link
16. (20 de septiembre de 2019), Presentan proyecto de Ley de Protección de Datos Personales, *Teleamazonas, 24 horas mediodía (13:28)*. Recuperado de link
17. (20 de septiembre de 2019), El ecuatoriano es dueño de su información según establece La Ley de Protección de Datos Personales, *Teleamazonas, 24 horas estelar*. Recuperado de link
18. Presentan Ley de Protección de Datos en Asamblea, (20 de septiembre de 2019), *Ecuavisa, Televistazo mediodía*. Recuperado de link
19. Carrión, Andrés, entrevistador (22 de septiembre), La Ley de Protección de Datos Personales prevé poner límites a comercialización de bases de datos, *Teleamazonas, Hora25 con Andrés Carrión*, Recuperado de link

20. (23 de septiembre de 2019), La Ley de Protección de Datos Personales prevé poner límites a comercialización de bases de datos, *Teleamazonas, Noticiero24Horas*, mediodía. Recuperado de link
21. Pinoargotte, Alfredo, entrevistador, (24 de septiembre de 2019), Hay que aplicar principios y responsabilidades en tratamiento de los datos personales, *Ecuavisa, Contacto Directo*, Recuperado de link
22. Valarezo, Luis, entrevistador, (26 de septiembre de 2019) La protección de datos personales es integral, *RTU canal*. Recuperado de link
23. Rodolfo Baquerizo, entrevistador (14 de octubre de 2019), El Ecuador debe tener una cultura de protección de datos, *Tc Televisión – Análisis*. Recuperado de link
24. (16 de octubre de 2019), Andrés Michelena Ayala: Ecuador debe contar con una Ley de Protección de Datos Personales, Televisión Legislativa, noticiero al mediodía. Recuperado de link
25. (19 de octubre de 2019), La Ley de Protección de Datos Personales llegó a la Asamblea Nacional, Televisión Legislativa, noticiero estelar. Recuperado de link

2.1.6 BOLETINES

2.1.6.1 Sitio institucional DINARDAP: http://www.datospublicos.gob.aec

1. Dirección de Comunicación Social. (04 de enero de 2019). La cultura de protección de datos personales es importante para los niños, niñas y adolescentes. Sitio institucional DINARDAP. Recuperado de link
2. Dirección de Comunicación Social. (04 de enero de 2019). Mesas de diálogo del Anteproyecto de Ley de Protección de Datos Personales concluyen este mes en Quito. Sitio institucional DINARDAP. Recuperado de link
3. Dirección de Comunicación Social. (07 de enero de 2019). Lorena Naranjo Godoy: "Protegiendo nuestros datos personales, nos protegemos a nosotros mismos". Sitio institucional DINARDAP. Recuperado de link
4. Dirección de Comunicación Social. (09 de enero de 2019). Las mesas de diálogo del anteproyecto de Ley de Protección de Datos personales se realizarán en Quito. Sitio institucional DINARDAP. Recuperado de link
5. Dirección de Comunicación Social. (15 de enero de 2019). La Ley de Protección de Datos Personales fortalecerá el uso de los datos personales. Sitio institucional DINARDAP. Recuperado de link
6. Dirección de Comunicación Social. (16 de enero de 2019). Mesas de diálogo para la construcción participativa del Anteproyecto de Ley de Protección de Datos Personales concluyeron en Quito. Sitio institucional DINARDAP. Recuperado de link
7. Dirección de Comunicación Social, (17 de enero de 2019, 11:37 am), La protección de datos personales en el Ecuador es fundamental para el desarrollo económico, digital y social. Sitio institucional DINARDAP. Recuperado de link

8. Dirección de Comunicación Social, (21 de enero de 2019, 11:49 am), Más actores sociales se suman a la construcción participativa del Anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de link
9. Dirección de Comunicación Social, (22 de enero de 2019, 4:25 pm), Entrevista: "Con una Ley de Protección de Datos Personales, se garantizan los derechos de los ciudadanos" – Diario Mercurio. Sitio institucional DINARDAP. Recuperado de link
10. Dirección de Comunicación Social, (25 de enero de 2019, 1:47 pm), Ministro de Telecomunicaciones destacó la importancia de una Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de link
11. Dirección de Comunicación Social, (4 de febrero de 2019, 1:19 pm), Una Ley de Protección de datos Personales permitirá enfrentar los desafíos de los avances tecnológicos. Sitio institucional DINARDAP. Recuperado de link
12. Dirección de Comunicación Social, (4 de febrero de 2019, 1:19 pm), Una Ley de Protección de datos Personales permitirá enfrentar los desafíos de los avances tecnológicos. Sitio institucional DINARDAP. Recuperado de link
13. Dirección de Comunicación Social, (30 de abril de 2019, 12:15 pm), En mayo, la Dinardap entregará anteproyecto de Ley de Protección de Datos Personales al Mintel. Sitio institucional DINARDAP. Recuperado de link
14. Dirección de Comunicación Social, (2 de mayo de 2019, 5:02 pm), La Protección de Datos Personales es fundamental para no afectar derechos. Sitio institucional DINARDAP. Recuperado de link
15. Dirección de Comunicación Social, (22 de mayo de 2019, 3:59 pm), La revisión final del Anteproyecto de Ley de Protección de Datos Personales se desarrollará en la Dinardap. Sitio institucional DINARDAP. Recuperado de link
16. Dirección de Comunicación Social, (23 de mayo de 2019, 5:02 pm), Revisión final del Anteproyecto de Ley de Protección de Datos Personales se efectuó en la Dinardap. Sitio institucional DINARDAP. Recuperado de link
17. Dirección de Comunicación Social, (11 de junio de 2019, 12:08 pm), La Ley de Protección de Datos previene que la información personal sea mal utilizada. Sitio institucional DINARDAP. Recuperado de link
18. Dirección de Comunicación Social, (21 de junio de 2019, 2:18 pm), La protección de datos personales es primordial en el Comercio Electrónico. Sitio institucional DINARDAP. Recuperado de link
19. Dirección de Comunicación Social, (21 de junio de 2019, 6:27 pm), La protección de datos personales es uno de los componentes que integrarán los Indicadores de Universalidad del Internet. Sitio institucional DINARDAP. Recuperado de link
20. Dirección de Comunicación Social, (24 de junio de 2019, 5:13 pm), La Dinardap inicia encuentros con asambleístas para dialogar sobre el anteproyecto de Ley Orgánica de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de link
21. Dirección de Comunicación Social, (25 de junio de 2019, 12:33 pm), Expertos destacan la importancia de la protección de datos personales en el Ecuador. Sitio institucional DINARDAP. Recuperado de link

22. Dirección de Comunicación Social, (25 de junio de 2019, 5:05 pm), Una Ley de Protección de Datos Personales promueve la creación de derechos digitales. Sitio institucional DINARDAP. Recuperado de link
23. Dirección de Comunicación Social, (26 de junio de 2019, 10:46 am), Asambleístas reciben seminario sobre el contenido y la importancia de una Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de link
24. Dirección de Comunicación Social, (26 de junio de 2019, 2:52 pm), La Dinardap trabajó más de un año en la construcción participativa del Anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de link
25. Dirección de Comunicación Social, (27 de junio de 2019, 3:37 pm), La protección de los datos personales depende del Estado y del ciudadano. Sitio institucional DINARDAP. Recuperado de link
26. Dirección de Comunicación Social, (5 de julio de 2019, 4:26 pm), Estudiantes de la Universidad UTE conocen sobre la importancia de proteger sus datos personales. Sitio institucional DINARDAP. Recuperado de link
27. Dirección de Comunicación Social, (9 de julio de 2019, 10:10 am), Jueces y abogados abordaron la importancia de los derechos digitales y la protección de datos personales. Sitio institucional DINARDAP. Recuperado de link
28. Dirección de Comunicación Social, (10 de julio de 2019, 3:05 pm), Dinardap capacitó a jueces y funcionarios judiciales sobre protección de datos personales. Sitio institucional DINARDAP. Recuperado de link
29. Dirección de Comunicación Social, (11 de julio de 2019, 9:31 am), Sector productivo conoció el Anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de link
30. Dirección de Comunicación Social, (12 de julio de 2019, 1:04 pm), La Dinardap trabaja en el anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de link
31. Dirección de Comunicación Social, (12 de julio de 2019, 4:42 pm), Lorena Naranjo Godoy: Cuando se utilizan datos personales, se trabaja con la identidad de los ciudadanos. Sitio institucional DINARDAP. Recuperado de link
32. Dirección de Comunicación Social, (23 de julio de 2019, 4:15 pm), El derecho de protección de datos personales está determinado en la Constitución. Sitio institucional DINARDAP. Recuperado de link
33. Dirección de Comunicación Social, 25 de julio de 2019, 4:13 pm), Iria Puyosa: Los periodistas deben conocer la importancia de la protección de datos personales. Sitio institucional DINARDAP. Recuperado de link
34. Dirección de Comunicación Social, (29 de julio de 2019, 4:47 pm), El Derecho en Ecuador debe tener un escenario digital. Sitio institucional DINARDAP. Recuperado de link
35. Dirección de Comunicación Social, (31 de julio de 2019, 10:24 am), Toda la información ciudadana debe ser resguardada por una Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de link

36. Dirección de Comunicación Social, (6 de agosto de 2019, 4:04 pm), El Anteproyecto de Ley de Protección de Datos Personales propende a evitar vulneraciones de derechos humanos. Sitio institucional DINARDAP. Recuperado de link
37. Dirección de Comunicación Social, (8 de agosto de 2019, 12:40 pm), Una normativa para la protección de datos personales debe ampararse en el respeto a los Derechos Humanos. Sitio institucional DINARDAP. Recuperado de link
38. Dirección de Comunicación Social, (14 de agosto de 2019, 10:03 am), El desarrollo de la tecnología debe ser simultáneo a la protección de los datos personales. Sitio institucional DINARDAP. Recuperado de link
39. Dirección de Comunicación Social, (21 de agosto de 2019, 5:01 pm), Dinardap y la Aepdp analizaron algunos temas del Anteproyecto de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de link
40. Dirección de Comunicación Social, (28 de agosto de 2019, 4:47 pm), La Seguridad Digital en empresas fomenta la cultura de protección de datos personales en sus usuarios. Sitio institucional DINARDAP. Recuperado de link
41. Dirección de Comunicación Social, (29 de agosto de 2019, 4:52 pm), Los datos abiertos fomentan la transparencia y no riñen con la protección de datos personales. Sitio institucional DINARDAP. Recuperado de link
42. Dirección de Comunicación Social, 29 de agosto d 2019, 5:06 pm, Ecuador quiere llegar a una protección de datos transparente. Sitio institucional DINARDAP. Recuperado de link
43. Dirección de Comunicación Social, (02 de septiembre de 2019, 10:12 am), Ecuador puede llegar a estándares internacionales en protección de datos personales. Sitio institucional DINARDAP. Recuperado de link
44. Dirección de Comunicación Social, (3 de septiembre de 2019, 12:56 pm), Una Ley de Protección de Datos Personales protege los derechos de la ciudadanía. Sitio institucional DINARDAP. Recuperado de link
45. Dirección de Comunicación Social, (13 de septiembre de 2019, 4:14 pm), Sociedad civil conoció el Anteproyecto de Ley de Protección de Datos Personales. Sitio institucional DINARDAP. Recuperado de link
46. Dirección de Comunicación Social, (16 de septiembre de 2019, 6:29 pm), Anteproyecto de Ley de Protección de Datos Personales irá a la Asamblea Nacional en 72 horas. Sitio institucional DINARDAP. Recuperado de link
47. Dirección de Comunicación Social, (19 de septiembre de 2019, 12:31 pm), La seguridad digital es una preocupación global. Sitio institucional DINARDAP. Recuperado de link
48. Dirección de Comunicación Social, (19 de septiembre de 2019, 4:55 pm), Lorena Naranjo Godoy: "Los ecuatorianos necesitamos derechos digitales". Sitio institucional DINARDAP. Recuperado de link
49. Dirección de Comunicación Social, (19 de septiembre de 2019, 4:58 pm), Proyecto de Ley de Protección de Datos Personales será entregado hoy. Sitio institucional DINARDAP. Recuperado de link

50. Dirección de Comunicación Social, (20 de septiembre de 2019 10:47 am), La educación digital es primordial para fomentar los derechos digitales. Sitio institucional DINARDAP. Recuperado de link
51. Dirección de Comunicación Social, (20 de septiembre de 2019, 2:57 pm), Las personas ya no somos solo físicas sino también virtuales. Sitio institucional DINARDAP. Recuperado de link
52. Dirección de Comunicación Social, (20 de septiembre de 2019, 4:37 pm), Lorena Naranjo Godoy: "Los ecuatorianos necesitamos derechos digitales". Sitio institucional DINARDAP. Recuperado de link
53. Dirección de Comunicación Social, (20 de septiembre de 2019, 4:45 pm), La ciudadanía debe exigir una Ley que proteja sus datos personales. Sitio institucional DINARDAP. Recuperado de link
54. Dirección de Comunicación Social, (20 de septiembre de 2019, 5:07 pm), La migración de datos al Data Center de CNT asegurará la información ciudadana. Sitio institucional DINARDAP. Recuperado de link
55. Dirección de Comunicación Social, (21 de septiembre de 2019, 1:12 pm), La Ley de Protección de Datos Personales impide el uso indebido de información. Sitio institucional DINARDAP. Recuperado de link
56. Dirección de Comunicación Social, (23 de septiembre de 2019, 11:27 am), Cultura de prevención se incluyen en el proyecto de Ley de Protección de Datos Personales". Sitio institucional DINARDAP. Recuperado de link
57. Dirección de Comunicación Social, (24 de septiembre de 2019, 10:54 am), Educación digital es la piedra angular para defender los datos personales". Sitio institucional DINARDAP. Recuperado de link
58. Dirección de Comunicación Social, (24 de septiembre de 2019, 11:14 am), En el Ecuador hay que trabajar en la construcción de la salud digital". Sitio institucional DINARDAP. Recuperado de link
59. Dirección de Comunicación Social, (24 de septiembre de 2019, 12:20 pm), Hay que implementar una serie de principios y responsabilidades en el tratamiento de los datos personales. Sitio institucional DINARDAP. Recuperado de link
60. Dirección de Comunicación Social, (24 de septiembre de 2019, 12:41 pm), Un manejo adecuado de los datos fideliza a los usuarios". Sitio institucional DINARDAP. Recuperado de link
61. Dirección de Comunicación Social, (25 de septiembre de 2019, 12:12 pm), Las bases de datos erróneas perjudican los derechos de los ciudadanos. Sitio institucional DINARDAP. Recuperado de link
62. Dirección de Comunicación Social, (25 de septiembre de 2019, 12:20) Las empresas deben garantizar un tratamiento adecuado de los datos personales de los ciudadanos. Sitio institucional DINARDAP. Recuperado de link
63. Dirección de Comunicación Social, (25 de septiembre de 2019, 12:27pm), El Proyecto de Ley de Protección de Datos Personales garantiza derechos. Sitio institucional DINARDAP. Recuperado de link

64. Dirección de Comunicación Social, (25 de septiembre de 2019 de 12:40 pm), Lorena Naranjo: “La Ley propuesta no es solo sobre seguridad, sino a una visión integral de la protección de datos”. Sitio institucional DINARDAP. Recuperado de link
65. Dirección de Comunicación Social, (25 de septiembre de 2019, 1:19 pm), Se puede aplicar buenas prácticas hasta que la Ley de Protección de Datos Personales se apruebe. Sitio institucional DINARDAP. Recuperado de link
66. Dirección de Comunicación Social, (26 de septiembre de 2019, 9:54 am), Una Ley de Protección de Datos Personales es esencial dentro de la era digital. Sitio institucional DINARDAP. Recuperado de link
67. Dirección de Comunicación Social, 26 de septiembre de 2019, 12:11 pm), El Proyecto de Ley de Protección de Datos Personales debe analizarse de manera urgente. Sitio institucional DINARDAP. Recuperado de link
68. Dirección de Comunicación Social, 26 de septiembre de 2019, 1:33 pm), La Ley de Protección de Datos Personales protege a residentes de diversas nacionalidades. Sitio institucional DINARDAP. Recuperado de link
69. Dirección de Comunicación Social, (26 de septiembre de 2019, 5:08 pm, La autoridad de control regulará y controlará el buen uso de los datos ciudadanos. Sitio institucional DINARDAP. Recuperado de link
70. Dirección de Comunicación Social, (27 de septiembre de 2019, 10:55 am), La educación digital es primordial para fomentar los derechos digitales. Sitio institucional DINARDAP. Recuperado de link
71. Dirección de Comunicación Social, (27 de septiembre de 2019, 11:06 am), El uso de datos personales contribuye a brindar mejores servicios a la ciudadanía. Sitio institucional DINARDAP. Recuperado de link
72. Dirección de Comunicación Social, (27 de septiembre de 2019, 11:58 am), El Ejecutivo determinará la institucionalidad de la entidad de control de datos personales. Sitio institucional DINARDAP. Recuperado de link
73. Dirección de Comunicación Social, (27 de septiembre de 2019, 12:01 pm), La sociedad es corresponsable de construir cultura de protección de datos personales. Sitio institucional DINARDAP. Recuperado de link
74. Dirección de Comunicación Social, (27 de septiembre de 2019, 4:39 pm), La seguridad digital significa cuidar los datos personales desde la misma ciudadanía. Sitio institucional DINARDAP. Recuperado de link
75. Dirección de Comunicación Social, (30 de septiembre de 2019, 10:07 am), Sin una Ley de Protección de Datos Personales no podemos desarrollar una cultura de protección digital. Sitio institucional DINARDAP. Recuperado de link
76. Dirección de Comunicación Social, (30 de septiembre de 2019, 1:14 pm), Los principios de la Ley de Protección de Datos Personales evitan la suplantación de identidad. Sitio institucional DINARDAP. Recuperado de link
77. Dirección de Comunicación Social, (30 de septiembre de 2019, 1:21 pm), “Los datos personales somos nosotros mismos, por ello hay que cuidarlos”. Sitio institucional DINARDAP. Recuperado de link
78. Dirección de Comunicación Social, (30 de septiembre de 2019, 6:34 pm), Para proteger los datos personales hay que educar digitalmente Para proteger los datos

personales hay que educar digitalmente. Sitio institucional DINARDAP. Recuperado de link
79. Dirección de Comunicación Social, (04 de octubre de 2019, 12:00 pm), Especialistas destacaron la importancia de una Ley de Protección de Datos Personales, Sitio institucional DINARDAP. Recuperado de link
80. Dirección de Comunicación Social, (01 de octubre de 2019, 16:23) La seguridad de los datos personales es integral. Sitio institucional DINARDAP. Recuperado de link
81. Dirección de Comunicación Social, (01 de octubre de 2019, 15:46), "Todos debemos construir en una cultura de protección de datos personales". Recuperado de link

2.6.1.2 Sitio institucional MINTEL: https://www.telecomunicaciones.gob.ec

1. Dirección de Comunicación Social. (17 de enero de 2019). MINTEL participó en las mesas de diálogo para la construcción del anteproyecto de Ley de Protección de Datos Personales. Sitio institucional MINTEL. Recuperado de link

2. Dirección de Comunicación Social. (29 de enero de 2019). MINTEL trabaja por la protección de datos de los ecuatorianos. Sitio institucional MINTEL. Recuperado de link

3. Dirección de Comunicación Social. (28 de marzo de 2018). Dinardap incluye a actores relacionados con proyecto de Ley de Protección de Datos Personales, para recibir sus aportes. Sitio institucional MINTEL. Recuperado de link

4. Dirección de Comunicación Social. (07 de junio de 2018). MINTEL socializó los resultados de las mesas de trabajo territoriales para la construcción del PSIC. Sitio institucional MINTEL. Recuperado de link

5. Dirección de Comunicación Social. (16 de septiembre de 2019). Gobierno enviará a la Asamblea Nacional, Ley de Protección de Datos Personales. Sitio institucional MINTEL. Recuperado de link

6. Dirección de Comunicación Social. (17 de septiembre de 2019). Ministro Michelena anunció traslado de toda la información gubernamental al Data Center de la CNT. Sitio institucional MINTEL. Recuperado de link

7. Dirección de Comunicación Social. (19 de septiembre de 2019). Ministro Michelena entregó proyecto de Ley Protección de Datos Personales al presidente de la Asamblea Nacional. Sitio institucional MINTEL. Recuperado de link

8. Dirección de Comunicación Social. (24 de septiembre de 2019). Ecucert denuncia ante Fiscalía posible exposición de datos personales. Sitio institucional MINTEL. Recuperado de link