El Delegado de Protección de Datos Personales, mecanismo idóneo para la protección de los usuarios de las entidades privadas en clave a la recolección, tratamiento y uso de sus datos personales en Colombia.

Autores

Montealegre Rodríguez Linda Nathaly (Cód. 42162045)

Vargas Rojas Andrés David (Cód. 42162190)

Asesor

David Mendoza Beltrán

Monografía De Investigación

Universidad Libre

Facultad de Derecho

Centro de Investigaciones Sociojurídicas

Bogotá D.C

2021

Agradecimientos

A Dios, por dotarnos de las capacidades necesarias para hacer esto posible; a nuestras familias por su apoyo incondicional y a nuestro amor mutuo que nos ayuda a superar con coraje cada reto que nos pone la vida.

Aceptación

(Con la calificación y valoración del Asesor(a) o evaluador (validación o aprobación extraordinaria del CUA). Para el momento de la sustentación como Opción de Grado, esta página estará destinada para el Jurado).

Valoración:_____

_____

_____

_____

_____

_____

_____

_____

_____

Calificación (A o I): _____

_____

Dr. (a)

Jurado (o Asesor)

_____

Dr. (a)

Jurado

_____

Dr. (a)

Jurado

Autoridades académicas

Presidente

Dr. Jorge Alarcón Niño

Vicepresidente

Dr. Jorge Gaviria Liévano

Rector Nacional

Dr. Fernando Enrique Dejanón Rodríguez

Secretario General

Dr. Floro Hermes Gómez Pineda

Censor Nacional

Dr. Ricardo Zopó Méndez

Presidente Seccional

Dra. Elizabeth García González

Rector Seccional

Dr. Fernando Arturo Salinas Suárez

Decano

Dr. Luis Francisco Ramos Alfonso

Secretaría Académica

Dra. Ana Rocío Niño Pérez

Coordinador Académico Campus El Bosque Popular

Dr. Alejandro Arévalo Gómez

Director centro de investigaciones sociojurídicas

Dr. Gustavo José Rojas Pérez

Directora Consultorio Jurídico

Dra. Mabel Bonilla Correa

Coordinadora Consultorio Jurídico Campus El Bosque Popular

Dra. Janeth Callejas Cifuentes

Coordinador Área De Investigación

Dr. Belisario Daza González

Tabla de contenido

Tabla de gráficas

Tabla de cuadros

Introducción

La presente investigación se desarrolla con base en el manejo indebido e inadecuado que las empresas colombianas de carácter privado les dan a los datos personales de sus usuarios a partir del proceso de recolección, tratamiento y uso de datos personales, dando por resultado, la vulneración directa del derecho fundamental a la intimidad que se desglosa en los protección de datos personales y otros derechos afines como el derecho a la personalidad, al honor y a la vida privada y el Habeas Data.

En Colombia se evidencia a través de estudios, análisis y actos administrativos emitidos por la Superintendencia de Industria y Comercio -SIC-, que las empresas privadas carecen de mecanismos de control eficientes para garantizar la tutela efectiva del derecho fundamental a la protección de datos personales, adicional a esto, los informes entregados por la Fiscalía General de la Nación indican, de una manera desalentadora, que las trasgresiones a este derecho solo van en aumento, pues cada vez se allegan más noticias criminales relacionadas con el delito de violación de datos personales.

Conforme a lo anterior, se formuló la siguiente pregunta de investigación: ¿Cómo se puede lograr la materialización de la legislación referente a la protección de datos personales para evitar la vulneración de los derechos de los usuarios de las entidades privadas?

El Delegado De Protección de Datos -DPD-, entendido como el mecanismo garantista, enmarca un papel determinante para blindar y garantizar los derechos fundamentales en cuestión, como quiera que, a ojos de la eficacia, este representa un eje central en cuanto a la rendición de

cuentas, ya que actúa como regulador independiente al interior de cada entidad favoreciendo así la materialización de la normativa vigente y de los mecanismos establecidos en ella. Para esto, se ve la necesidad de introducir la figura de DPD en nuestro ordenamiento jurídico, con la finalidad de salvaguardar el derecho fundamental a la protección de datos personales que es, en últimas, el propósito de esta investigación.

Utilizando el punto de vista del enfoque funcionalista, se analizó la perspectiva nacional e internacional de la protección de datos personales en cuanto a su regulación y mecanismos; del mismo modo, se analizaron las vertientes estadounidense y europea. Lo anterior para vislumbrar como mecanismo garantista del derecho a la protección de datos personales al Delegado de Protección de Datos.

Se planteó como objetivo general, describir la necesidad de integrar al Delegado De Protección De Datos al ordenamiento jurídico vigente, como mecanismo garantista del derecho fundamental a la protección de datos personales en clave a la recolección, tratamiento y uso de datos al interior de las empresas de carácter privado, con la finalidad de lograr la eficacia material de las disposiciones normativas que cobijan este derecho.

Para efecto de lo anterior, se proyectaron como objetivos específicos: i) analizar, con base en las denuncias, estudios y providencias de la Superintendencia de Industria y Comercio, las violaciones al derecho fundamental a la intimidad y conexos por el uso, recolección y tratamiento indebido o arbitrario de los datos personales de particulares por parte de entidades privadas; ii) explicar el aporte del DPD a la efectiva garantía del derecho fundamental a la protección de datos personales, teniendo en cuenta los procesos a los que son sometidos y que se realiza por parte de las empresas privadas, sin tener en cuenta las obligaciones consagradas en el marco legal y; iii)

describir la importancia de favorecer el principio de seguridad en relación con el DPD para contrarrestar el indebido e inadecuado uso de los datos por parte de las empresas privadas en el proceso de recolección uso y tratamiento de los mismos.

La presente monografía se adscribe a la línea de investigación de carácter socio jurídico en el ámbito del derecho privado, en cuanto a la protección de datos personales y su efectiva protección, así propendiendo por la estructuración de un mejor país en aras de enaltecer la sociedad democrática, pluralista, tolerante y cultora de la diferencia que nos identifica.

Este estudio se caracteriza por ser una investigación sociojurídica, en la que se adecuo el enfoque funcionalista, a través del análisis de distintos ordenamientos jurídicos, por medio del cual se realizó la recolección de alternativas jurídicas en torno a la prevención y protección de los datos personales que han sido adoptadas por diferentes países en el mundo. Para lograr lo anterior, se realizó una observación investigativa comparada frente a ordenamientos jurídicos ajenos a Colombia, haciendo énfasis en la Unión Europea y Norteamérica. Del mismo modo, para garantizar la aplicación efectiva del principio de seguridad, se debe hacer uso de la figura del Delegado de Protección de Datos para que, a través de esta, se asegure el cumplimiento de las disposiciones instauradas en la legislación vigente en torno a la salvaguarda de la información personal y el derecho en cabeza de los usuarios de entidades privadas.

En un inicio, el primer capítulo ahonda la situación por la cual se está vulnerando el derecho a la protección de datos personales de los usuarios de entidades privadas, producto del manejo indebido e inadecuado de los datos personales en el proceso de recolección, tratamiento y uso de la información personal para que, subsiguientemente, se realice un paneo acucioso respecto de la regulación normativa colombiana que cobija el actual derecho vulnerado, llegándose a la

conclusión de que la misma cuenta con desaciertos legislativos y carece de figuras preventivas efectivas en cuanto a la recolección uso y tratamiento de los datos. Al mismo tiempo, se hizo un recorrido histórico de la protección de datos personales, estableciendo de manera específica las situaciones problema, a partir del funcionalismo. Por otra parte, se realizó un análisis critico del principio fundamental de la protección de datos personales, resaltando su importancia y características. Finalmente, se estableció, a partir de conceptos críticos de autores que los mecanismos de control y vigilancia orientados a la protección de datos deben propender por una efectiva garantía de los intereses tanto individuales como colectivos al momento del procesamiento de datos.

En el segundo capítulo, se lleva a cabo el desarrollo del método, esto es, la recolección de alternativas jurídicas en torno a la prevención y protección de los datos personales que han sido optadas por los diferentes países del mundo, teniendo en cuenta: i) la perspectiva nacional de la protección de datos personales; ii) la regulación internacional en materia de protección de datos personales; iii) los mecanismos internacionales para la protección de datos personales; iv) las vertientes estadounidense y europea, ¿cuál es la mejor para Colombia? Y; v) el mecanismo: Delegado de Protección de Datos -DPD-, una visión garantista para la prevención en materia de protección de datos en Colombia. Por consiguiente, agrupada y analizada la información de manera rigurosa, se toma al Delegado de Protección de Datos, como aquel mecanismo decisivo a implementar en la legislación colombiana, en aras de garantizar la observancia y el respeto por las leyes actuales en materia de protección de datos en relación a la recolección, tratamiento y uso de la información, así permitiendo la garantía de los derechos fundamentales a la intimidad, la personalidad, al honor y a la vida privada y el Habeas Data.

El tercer capítulo, desarrolla, la necesidad de implementación del Delegado de Protección de Datos, basándose en las problemáticas actuales de efectividad que se encuentran en la norma y la realidad jurídica de las empresas privadas. Al mismo tiempo se establece que el principio o regla que se quiere privilegiar en las prácticas profesionales del derecho es el principio de seguridad, enmarcado en el ámbito legal en la ley 1581 de 2012. Por el mismo entramado, se quiere dar respuesta al problema jurídico de investigación a raíz de los argumentos de los expertos consultados, realizando una fundamentación teórica para validar de manera cualitativa la necesidad de implementar el Delegado de Protección de Datos, para obtener una mayor efectividad frente a lo prescrito por los mandatos constitucionales del derecho a la intimidad y conexos.

Como resultado de la presente investigación, debe precisarse que, las actuaciones de una empresa de carácter privado en cuanto la recolección, tratamiento y uso no deben ser encaminas a la transgresión de derechos fundamentales, si no propender por el cumplimiento del marco regulatorio actual, esbozando la necesidad de aclarar, regular e implementar mecanismos de control para garantizar la eficacia de dichas actividades y así salvaguardar los intereses tanto individuales como colectivos de los sujetos objeto de derecho.

A la luz del principio de seguridad, debe existir un marco legal donde se introduzca la figura del Delegado de Protección de datos, para así lograr la materialización eficaz de las disposiciones y mecanismos establecidos en el ordenamiento jurídico colombiano para la protección de los datos personales como derecho fundamental inherente a los usuarios de las organizaciones de carácter privado.

Capítulo I

La Superintendencia de Industria y Comercio de Colombia como ente de autoridad en el ámbito de la protección de datos personales anunció el 11 de marzo de 2021, en su segundo análisis anual referente a las medidas de seguridad, que más de 24.424 organizaciones en Colombia carecen de mecanismos efectivos para salvaguardar la información personal de sus usuarios de accesos no autorizados, pues no han puesto en práctica las políticas de protección pertinentes. Adicional a esto, se descubrió que 20.594 empresas no han llevado a cabo la implementación de políticas específicas en relación al acceso a la información personal relacionada con datos sensibles; cifras que permiten evidenciar que en Colombia hay un déficit en torno a la aplicación de los mecanismos establecidos por la ley para la protección de los datos personales, como figura que garantiza el tratamiento seguro y adecuado de la información (Superintendencia de Industria y Comercio, 2021).

Cuadro No. 01

Resultados del estudio de seguridad del año 2020 elaborado por la SIC

	2020
Número de organizaciones evaluadas	33.596
No tienen una política de protección para acceso remoto a la información personal	72.7%
No cuenta con mecanismos de monitoreo de consulta de las bases de datos	69.3%
No ha implementado un procedimiento de auditoría de los sistemas de información	71.3%
No tiene implementado un sistema de gestión de seguridad o un programa integral de gestión de datos	67.5%
No ha implementado medidas especiales para proteger datos sensibles	61.3%
No ha implementado una política de seguridad para el intercambio físico o electrónico de datos	66.1%
No tiene política de auditoria de seguridad de la información	63.6%
No tiene controles de seguridad en la tercerización de servicios para el tratamiento de datos	61%
No implementa medidas apropiadas y efectivas de seguridad	50.7%
No cuenta con herramientas de gestión de datos	49.9%
No tiene políticas y procedimientos de gestión de incidentes de seguridad	52.6%
Promedio de incumplimiento respecto de los ítems evaluados	**62.36%**

Recuperado de: "Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales" por Superintendencia de Industria y Comercio. 2021. https://www.sic.gov.co/

Las cifras y conclusiones expuestas en el cuadro anterior se han extraído de la información proporcionada por 33.596 entidades Responsables del Tratamiento de datos que realizaron el registro de sus bases de datos en la Superintendencia de Industria y Comercio (SIC) del año 2015 al 30 de septiembre del año 2020, de las cuales el 93.3% son empresas privadas (Superintendencia de Industria y Comercio, 2021).

Adicionalmente, y a manera de ejemplo, se advierte en actos administrativos como el 45743 de 2018 expedido por la SIC, entre muchos otros, la ejecución reiterada de conductas violatorias que derivan en la vulneración directa del derecho a la protección de datos personales y otros derechos afines, como tratar los datos personales de los usuarios sin solicitar su autorización previa para dicho tratamiento, contrariando así los deberes que le asisten como responsable del tratamiento de los datos y vulnerando uno de los principios rectores para el tratamiento de los mismos, como lo es el principio de libertad (Ministerio De Comercio, Industria y Turismo, Superintendencia De Industria y Comercio, Resolución 45743, 2018).

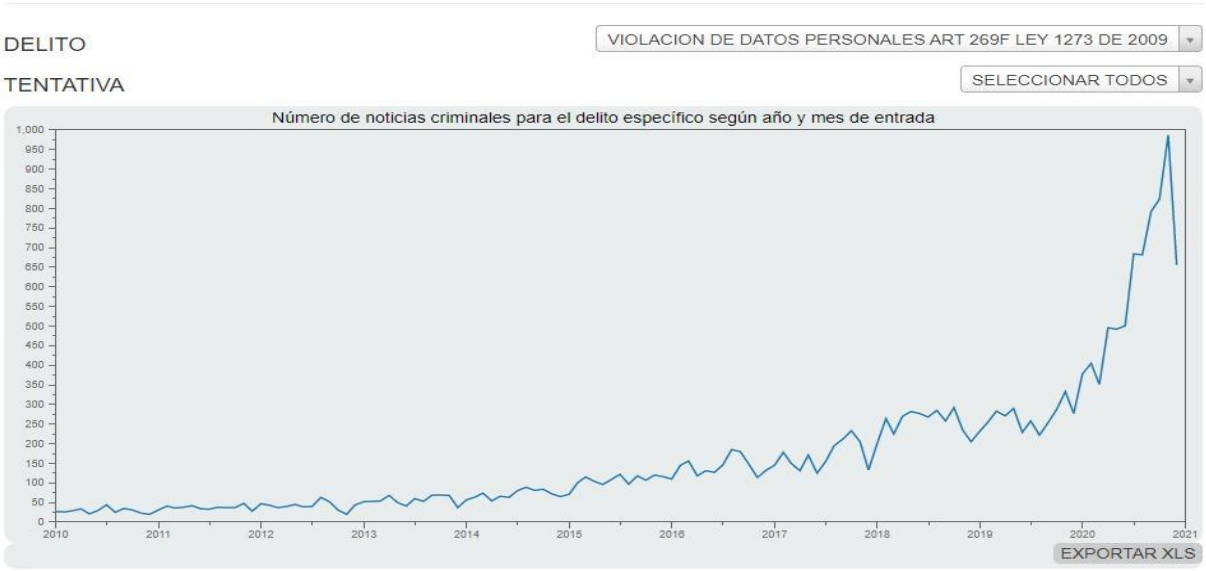
Por otra parte, es evidente que la realización de conductas que vulneran la protección de datos personales está trascendiendo, incluso, a la esfera de lo penal; pues según cifras suministradas por la Fiscalía General de la Nación, se evidencia que durante la última década ha crecido de manera exponencial y alarmante la tendencia a llevar a cabo prácticas que conducen a la violación directa e indirecta de los datos personales a través de su recolección, tratamiento y uso de manera indebida o fraudulenta.

La gráfica No. 01 representa la cantidad de noticias criminales relacionadas con la violación de datos personales (Artículo 269F – Ley1273 de 2009) recibidas por parte de la Fiscalía

General de la Nación en los últimos 10 años, donde se puede apreciar el aumento acelerado y vertiginoso de delitos relacionados con la vulneración de datos personales.

Gráfica No. 01

Número de noticias criminales para el delito de violación de datos personales en la última década



Fuente: Fiscalía General de la Nación. (2021). *Entradas de noticias criminales por delito en Ley 906 de 2004 y Ley 1098 de 2006.* [Gráfica]. Recuperado de https://www.fiscalia.gov.co

De lo anterior, se establece que han venido en aumento la comisión de conductas delictivas encaminadas a la vulneración del derecho fundamental a la protección de datos personales y por ende el desconocimiento de los presupuestos legales instaurados con la finalidad de evitar que los datos personales sean objeto de usos indebidos; muestra de ello es que tal y como lo refleja la gráfica, en el año 2010 el número de noticias criminales referentes a la violación de datos personales recibidas por la Fiscalía fue de trescientas cuarenta y cinco (345), cifra que para el año

2015 ya se había triplicado y que para el año 2020 alcanzó las siete mil doscientos cuarenta y ocho (7.248) noticias criminales relacionadas con dicha conducta; lo que resulta en un aumento de más del 2000%.

Podemos afirmar, entonces, que la protección de los datos personales se está viendo vulnerada en torno a las prácticas mediante las cuales se lleva a cabo su recolección, tratamiento y uso por parte de entidades públicas y privadas, siendo el caso de estas últimas el que atañe a la presente investigación; pues se ha dado lugar a la violación de distintos principios contemplados en la norma para dichas prácticas, produciendo así, una afectación directa a los usuarios de dichas entidades en cuanto a su derecho a la protección de los datos personales y otros derechos afines, como el derecho a la intimidad, a la personalidad, al honor y a la vida privada; todo esto a causa de la precaria eficacia del conjunto de normas expedidas por el legislador y los mecanismos de protección que estas contemplan, pues es claro que el tratamiento, recolección y uso de los datos personales de los usuarios de las entidades privadas no se está llevando a cabo de forma segura y acorde a la ley, ni se ha logrado garantizar que los mismos no sean objeto de usos indebidos.

Cabe considerar, además, que parte de la desprotección imperante sobre los datos personales y su tratamiento se debe a que el legislador ha ignorado el hecho de que al momento de la aplicación del derecho a la protección de datos personales es necesario tener en cuenta las nuevas tecnologías de la información, ya que por medio de estas se logra una captación masiva de información y gran parte de esta información son los datos personales de los individuos, lo que supone un inminente riesgo al tratamiento y uso indebido de los mismos (García, 2007).

Contexto normativo de la protección de datos personales

El derecho fundamental a la protección de datos personales cuenta en Colombia con diversos preceptos constitucionales, legales y jurisprudenciales que han sido desarrollados por distintas autoridades y órganos del ordenamiento jurídico colombiano.

Por su parte, la Constitución Política de 1991 contempla en su artículo 15, la recolección y tratamiento de datos personales siempre y cuando se respete la libertad y derechos consagrados en esta Carta Política, destacando su rango de derecho constitucional; posteriormente, la Ley Estatutaria 1581 de 2012 se encargó de regular la protección de datos personales como derecho fundamental, haciendo énfasis en que esta desarrollará los lineamientos necesarios para que los individuos tengan la posibilidad de "(…) conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos" (Ley Estatutaria 1581, 2012).

Dentro de este marco, la Honorable Corte Constitucional en sentencia C-748 de 2011 estableció, en su contenido fáctico y motivo, que la protección de datos personales debe tratarse como un derecho fundamental y a su vez se ha venido desarrollando como un derecho a la autodeterminación informática o derecho del habeas data, que si bien es cierto se desarrolla como un derecho autónomo, garantiza el desarrollo de otros derechos, tales como: la intimidad, el buen nombre y el libre desarrollo de la personalidad (Corte Constitucional, Sentencia C-748, 2011).

Además, el legislador en busca de evitar la transgresión de este derecho fundamental añade, con la Ley 1273 de 2009, los siguientes tipos penales: "acceso abusivo a un sistema informático, interceptación de datos informáticos, daño informático, violación de datos personales, suplantación de sitios web para capturar datos personales, entre otros" (Ley 1273, 2009).

Por la misma vía, el Decreto 1377 de 2013, en su artículo 4, concuerda con el alcance penal que se ha ido desarrollando a raíz de la vulneración del derecho a la protección de datos personales. Es por esto que señala que no se podrá llevar a cabo la utilización de medios engañosos o fraudulentos para la recolección de datos personales y, mucho menos, sin que exista de por medio autorización del titular de la información (Decreto 1377, 2013).

Todas las normas afines a garantizar y salvaguardar los intereses tanto individuales como colectivos que hacen alusión a la recolección, tratamiento y uso de la información de índole personal, convergen en lo relacionado al contenido de los artículos 17 y 18 de la Ley Estatutaria 1581 de 2012. En esta disposición legal que regula derechos fundamentales, se consagran los deberes de los responsables y encargados del manejo de los datos personales como, por ejemplo, "garantizar a su titular que, en todo tiempo, pueda disponer del pleno y efectivo ejercicio del derecho de habeas data" (Ley Estatutaria 1581, 2012, art.17).

Dentro de este orden de ideas, la Resolución 76434 de 2012, expedida por el Ministerio de Comercio, Industria y Turismo, contempla la manera en que debe circular la información y los deberes de los operadores, además, señala que se deberá aportar un manual interno con política y procedimientos para garantizar el adecuado cumplimento de la ley (Ministerio De Comercio, Industria y Turismo, Resolución 76434, 2012).

Es menester señalar que, cuando no se dé cumplimiento de los principios y garantías constitucionales por una determinada entidad al momento de usar y tratar los datos personales, la misma entidad deberá adelantar el proceso pertinente al caso, justo como lo ha reiterado la Corte Constitucional en la Sentencia C-748 de 2011. Siguiendo el mismo entramado, el Consejo de

Estado, Sala Contenciosa, en sentencia número 23001-23-33-000-2015-00506-01 de 2016, afirmó lo dicho por la Corte Constitucional y estableció que:

> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. Del contenido del precepto constitucional contenido en el artículo 15, se observa la consagración de tres derechos fundamentales autónomos, a saber, intimidad, buen nombre y habeas data, cuyo contenido si bien tiene estrecha relación, tienen sus propias particularidades (Consejo de Estado, Sentencia 23001-23-33-000-2015-00506-01, 2016).

La Ley 1581 de 2012, por su parte, limitó a las entidades encargadas de la recolección de datos, señalando lo siguiente:

> 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 y; d) la identificación, dirección física o electrónica y teléfono del responsable del tratamiento (Ley 1581, 2012, art.12).

Así mismo, el Decreto 1377 de 2013, en el artículo 13, señala que es el recolector de datos el encargado desarrollar las políticas para el tratamiento de estos y de velar por el cumplimiento de dichas políticas.

Cabe señalar que, si bien, implementar las nuevas tecnologías en el campo de la protección de datos personales es un desafío constante para el Estado, el Decreto 1377 de 2013 estipuló, en su artículo 16, que para el almacenamiento de datos se deberán desarrollar las políticas públicas

de tratamiento de la información y acceso a esta, empleando medios informáticos, electrónicos o cualquier otra tecnología.

De acuerdo con el artículo 26 del Decreto 1377 de 2013, "los encargados del tratamiento de la información deberán ser capaces de demostrar que han implementado las medidas apropiadas y efectivas para el cumplimiento de las obligaciones establecidas en la ley". Asimismo, establece el artículo 18 de la ley 1581 de 2012 que "los encargados del tratamiento de datos personales tienen por obligación garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data e informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares" (Ley 1581, 2012, art.18).

En definitiva, es clara la existencia de un desacierto legislativo en lo relacionado al tratamiento y recolección de datos personales por la efímera labor del Estado colombiano para lograr ser suficientemente garantista en cuanto a la materialización de las disposiciones normativas; si bien es cierto que, este derecho fundamental está consagrado en la Constitución Política, en algunos de las preceptos legales del ordenamiento jurídico y en la jurisprudencia, no es menos cierto que, no se ve reflejada la aplicabilidad por el mal uso de entidades públicas y privadas de los datos personales de los habitantes del país, transgrediendo su intimidad y demás derechos concordantes.

Recorrido histórico de la protección de datos personales

La evolución constante de la humanidad y la tecnología en los siglos contemporáneos denotan la necesidad de inmiscuirse en la era digital y de las telecomunicaciones, en donde el manejo, intercambio y transferencia de datos personales son mecanismos usados a diario, cuya

participación la ostentan los Estados, las sociedades cualquiera sea su razón social, las mismas personas naturales, entre otros. Lo anterior, con el ánimo de, sobretodo, obtener bienes, productos o servicios; asimismo, este tipo de prácticas conllevan a la necesidad de establecer una eficaz protección por tratarse de tan susceptible información, como lo son, los datos personales y debe realizarse, por un lado, por la administración pública y, por otro, por el ordenamiento jurídico.

El tratamiento de datos, históricamente, se ha realizado en épocas no tan antañas. Se remonta al siglo XX, en donde se implementaron con la ayuda de técnicas y herramientas informáticas, como se realizó en el año de 1943, donde un grupo de expertos al servicio del ejército británico fabricó el llamado *Colossus*, cuya finalidad era la de descifrar mensajes ocultos de los nazis durante la II Guerra Mundial. Además, en 1954, Estados Unidos también fue partícipe en los inicios del manejo de datos, por ejemplo, una cadena de televisión llamada CBS empleó un ordenador para realizar predicciones presidenciales; también la multinacional General Electric compra un ordenador UNIVAC (Universal Automátic Calculador) para llevar a cabo el procesamiento de información contable. También, en 1968 International Business Machines Corporation introdujo el primer sistema encargado de gestionar bases de datos, obteniendo un cúmulo significativo de datos técnicos y personales (Delgado y Pérez, 2010). Sin embargo, el tratamiento informático de datos se multiplicaba exponencialmente y, como consecuencia, existía la posibilidad de vulnerarse derechos fundamentales, como la intimidad o privacidad de las personas.

En la Unión Europea, los Estados miembros siembran una preocupación por la protección de los datos personales de los europeos. Siendo así, en el año de 1983 el Tribunal Constitucional Federal Alemán dio origen a la Ley del Censo, cuya finalidad era la regulación del derecho a la personalidad, a la dignidad humana, a la intimidad, a la autodeterminación informativa y al libre

desarrollo de la personalidad, derechos que son los pilares fundamentales para la protección de esta clase de datos. Sin embargo, antes de tan relevante Ley, existieron instrumentos normativos dedicados a la salvaguarda parcial de los datos personales, verbigracia, la Resolución 509 de 1968 expedida por el Consejo de Europa, que trataba sobre los derechos humanos y tenía como prioridad resguardar la privacidad de las personas ante la inminente ola tecnológica (Bejarano, 2014). A raíz de esta preocupación, son los Estados y las entidades del sector público en general quienes asumen el papel de guardianes de los datos personales.

Los Estados Unidos de América no fueron ajenos a esta preocupación, en 1974 tuvo lugar la expedición de la primera Ley de carácter general denominada "Privacy Act", que se orientaba a la protección de datos personales, estableciendo la obligación de que el titular de los datos, de manera expresa, otorgue su consentimiento para que se puedan tratar estos. Posteriormente, con el auge del internet en la década de los 90s se estructura un fenómeno mundial en el que los datos personales circulaban con una regulación precaria frente a su protección (Bejarano, 2014; Delgado, 2010). Lo anterior supone que, con los avances tecnológicos, la protección de datos personales debe ser un asunto de regulación jurídica nacional e internacional.

En Colombia, la necesidad de regular el tratamiento, manejo y transferencia de datos se reflejó, en principio, por la Constitución Política de 1991, en su artículo 15, en donde se blinda el derecho a la intimidad personal y familiar, al buen nombre, a la protección de datos personales, entre otros. Adicional a esto, la Ley 1266 de 2008, por la cual: "se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales (…)", reguló el mecanismo constitucional que tienen las personas para garantizar su defensa en aquellas situaciones en que su información personal pueda verse comprometida. Sin embargo, la eficacia tanto del conjunto de normas expedidas por el legislador, como el alcance

constitucional de estas, en aras de salvaguardar los derechos fundamentales de las personas sujetas a manipulación de datos es precaria, no existe una verdadera materialización de las normas en torno a la protección de datos por parte del Estado colombiano a lo largo de la historia.

La protección de datos personales como derecho fundamental

Como garantía de la protección de múltiples derechos y libertades inherentes a los individuos que forman parte del conglomerado social, la protección de datos personales como derecho fundamental impone una serie de deberes legales a cargo de las entidades privadas que llevan a cabo la recolección, tratamiento y uso de los datos personales, encaminados a salvaguardar los derechos e intereses de sus titulares; sin embargo, de las actuaciones de dichas entidades se puede vislumbrar su desconocimiento a los presupuestos legales instaurados para regular su proceder en cuanto al tratamiento de los datos de los usuarios, lo que nos lleva a concluir que no están funcionando de manera eficaz los mecanismos y herramientas contenidos en la normativa referente a la protección de datos personales. Por consiguiente, tenemos que el análisis que atañe a la presente investigación responde a un enfoque funcionalista, mediante el cual se proyecta la necesidad de realizar una actualización de los elementos y herramientas tanto legales como tecnológicos.

La protección de datos personales es definida como un derecho fundamental que no obstante gozar de autonomía, comporta a su vez la protección de otros derechos afines, como el derecho a la intimidad, la personalidad, el honor y la vida privada, entre otros, relacionados con el tratamiento de la información personal de los individuos que puede reposar en distintas fuentes y cuya salvaguarda le compete al Estado. (García, 2007; Hernández, 2012; Maqueo, Moreno & Recio, 2017; Meraz, 2018.) Por otra parte, Martínez (2007) considera que la protección de datos

personales debe entenderse como un instrumento o medio de control para amparar derechos y libertades.

La totalidad de los autores traídos a colación concuerda en el hecho de que la existencia de la protección de los datos personales surge por una razón plenamente garantista, toda vez que busca la protección de los derechos y libertades del individuo y a su vez los del conglomerado social al cual pertenece, evitando que los datos personales del sujeto sean objeto de usos indebidos por parte de las entidades encargadas del tratamiento de los mismos, allí radica la importancia de este derecho, en la salvaguarda que pretende brindar ante vulneraciones directas a los derechos del individuo en lo atiente al tratamiento de su información personal.(García,2007; Martínez, 2007; Hernández, 2012; Maqueo, Moreno & Recio 2017; Meraz,2018).

Al momento de la aplicación del derecho de protección de datos personales es necesario tener en cuenta las nuevas tecnologías de la información, ya que por medio de estas se logra una captación masiva de información, gran parte de esta información son los datos personales de los individuos, por lo que supone un inminente riesgo al tratamiento y uso indebidos de la información de estos mismos (García, 2007; Hernández, 2012; Meraz, 2018). Por otra parte, Martínez (2007) analiza desde otra perspectiva, diciendo que lo más importante a tener en cuenta al momento de la aplicación del derecho son las autoridades de control de los datos personales, ya que estas juegan un rol informativo, que es esencial para que el individuo conozca los derechos que le asisten y así no permitir que estos les sean vulnerados. Desde otra perspectiva, la protección de datos personales debería adoptar estándares comunes entre países para su aplicación, ya que los niveles de protección requeridos por un país difieren de los requeridos por otro, afectando la seguridad jurídica e igualdad de las personas, además entorpeciendo el flujo de información entre países (Maqueo, Moreno & Recio, 2017).

Dada su relevancia en el mundo actual por su relación con las nuevas tecnologías, la protección de datos personales, cuenta en la mayoría de países con el reconocimiento como derecho fundamental y la regulación normativa respectiva como respaldo; sin embargo, más allá del papel, los mecanismos para hacer efectiva la puesta en práctica de la norma y la garantía que ella significa para la salvaguarda de los derechos de los individuos resultan insuficientes, toda vez que no van al paso de los avances tecnológicos y esto desemboca en una serie de vulneraciones y abusos por parte de entidades de carácter público y privado relacionadas con la recolección, uso y tratamiento de datos personales .(García,2007; Martínez, 2007; Hernández, 2012; Meraz,2018). Abordando el tema desde otro ángulo Maqueo, Moreno y Recio (2017) hacen referencia a que pese al rápido avance de la tecnología, la inminente globalización que ha invadido la esfera de las relaciones humanas y la universalidad que envuelve el derecho a la protección de datos personales (al encontrarse incluido en la categoría de los derechos humanos) aún no existen estándares comunes de protección de datos entre los países del mundo.

De conformidad con la aplicación diversa de la protección de datos personales como derecho, esta funciona como un limitante al ejercicio del derecho a la libre expresión e información, ya que al momento de hacerse pública una opinión se debe tener en consideración los datos íntimos de un tercero con el fin de no vulnerar sus derechos (Martínez, 2007). Por otro lado, la protección de datos personales se aplica a modo de limitación para el comerciante de modo que para este surgen ciertas obligaciones para con el cliente u otro comerciante al momento de realizar actos de comercio, dicha obligación puede consistir entre otras cosas en preservar por diez años los documentos que contengan datos personales de la persona con la que se celebró el acto de comercio (Meraz, 2018). A partir de otra mirada, la aplicación del derecho a la protección de datos personales, se materializa a través del poder que puede tener una persona respecto de sus

datos con el objetivo de proteger otros derechos que tiene a su favor tales como la libertad de culto, la libertad sexual, la libertad de pensamiento y su intimidad. (García,2007; Hernández, 2012; Maqueo, Moreno & Recio 2017).

En ese orden de ideas, la protección de datos personales es un derecho fundamental autónomo, relacionado con la protección de otros derechos afines y cuyo objetivo es garantizar la salvaguarda de los intereses tanto individuales como colectivos respecto de la recolección, tratamiento y uso de su información personal por parte de entidades públicas y privadas; además, es imprescindible a la hora de evitar la vulneración de los derechos y libertades de los individuos y posibilita el establecimiento de parámetros que permitan fortalecer su protección. Por otra parte es primordial tener en cuenta que las nuevas tecnologías de la información han obligado al mundo jurídico a solventar nuevas necesidades de los individuos respecto del tratamiento de su información y la protección de la misma, dado su poder en el mundo actual y el peligro que supone su uso indebido para los individuos. Cabe resaltar, por otro lado, que no obstante la presencia y reconocimiento de la protección de datos personales en la legislación de muchos países, los mecanismos e instituciones instaurados para su garantía no funcionan de manera adecuada y efectiva, pues se siguen desconociendo los parámetros legales instaurados para orientar la actividad de las organizaciones a cargo de procesar la información personal de los sujetos.

Y, por último, es conveniente señalar que la protección de datos personales puede ser empleada no solo como un poder sino también como un límite. Como un poder, respecto del titular de la información cuando este puede decidir qué aspectos de su vida y sus relaciones deben permanecer en el plano de lo privado. Y como un límite en lo que respecta al ejercicio de otros derechos, cuyo goce indebido o abusivo podría derivar en la vulneración de múltiples derechos de los demás individuos.

Los datos personales en torno a las alternativas para su tutela efectiva

La tipología privilegiada en la presente investigación se enfoca en la reparación, actualización y fortalecimiento del sistema jurídico que ya está creado, a través de dos principios de tipificación, el primero despliega una solución desde la reforma legislativa y estructural sobre protección de datos y la segunda, se centra en la actualización de los elementos y mecanismos en torno a la salvaguarda del derecho.

María Becerra, Mirta Navarro (2012) opinan que debe haber una restructuración para que las empresas o terceros puedan manejar datos ajenos de forma adecuada sin caer en un delito; de la misma forma, Sara Scola (2015) plantea la necesidad de revisar las leyes para identificar una aplicación directa de las reservas y evitar la violación a la protección de datos; en tal sentido, coinciden en el planteamiento de una reforma a las leyes existentes sobre protección de datos, ya que consideran que las que existen actualmente ofrecen muy pocas garantías y están desactualizadas.

Por su parte, Jennifer Alexandra Mendoza Morales (2015) plantea que la solución se debe enfocar en apoyar a las leyes existentes sobre el tema con diversas herramientas para así hacer más efectiva la protección sobre los datos personales de los individuos; por el mismo entramado, otros autores como Javier Jesús Aliño (2018) y Carmen Sánchez (2009), convergen en la idea de que se debe hacer una actualización de los elementos y herramientas tanto legales como tecnológicos; de un lado, Aliño afirma que se debe hacer una actualización de las plataformas tecnológicas y que de este modo se podrá descubrir el foco del problema, con ello coincide Sánchez, sin embargo, para esta autora la actualización debe ir enfocada en mayor medida a los mecanismos de protección.

De otra parte, Betsy Yohanna Ruiz (2016) y Lucero Galvis (2012) opinan de manera concordante, que se deben modificar las formas de utilización de los mecanismos encargados de la verificación del uso y adecuado tratamiento de los datos personales, y a su vez, incluir de forma más amplia preceptos constitucionales y jurisprudenciales que permitan tener de manera más clara cómo llevar a cabo el correcto uso y tratamiento de los datos, todo esto teniendo como base la ponderación de derechos para lograr una menor afectación.

Ahora bien, otros autores consideran que lo que debe hacerse es una reforma estructural a todas las entidades para que no atenten contra la protección de los datos personales y de la misma manera capacitar e informar a las autoridades respectivas para proteger los derechos a la intimidad y protección de datos teniendo en cuenta que el afectado principal siempre será el ciudadano; siguiendo este hilo, la autora Ana Isabel Herrán (2002) manifiesta que a su parecer la solución a la problemática planteada en relación a la vulneración del derecho a la protección de los datos personales consiste en suprimir el poder que ostentan ciertas entidades sobre los datos personales de terceros; en el mismo orden de ideas, Valeria Millanes (2017) añade que es sobre las entidades sobre quién debe recaer la obligación de velar por la protección de datos cuyos titulares son sus usuarios.

Para finalizar las autoras Lina Ornelas, Melissa Higuera (2013) opinan que se deben adecuar los mecanismos que dan prioridad a esquemas de autorregulación por parte de los sujetos a quienes se les aplica la norma.

Ahora bien, teniendo una mayor claridad sobre el contenido de los tipos y los aportes de los distintos autores traídos a colación, es menester establecer la continuidad dialéctica resultante de la tipificación elaborada a partir de los conceptos de los autores, y la misma consiste notablemente en que las investigaciones analizadas con anterioridad concuerdan en que es

fundamental entender que la vigilancia y control de los mecanismos orientados a la protección de los datos personales debe garantizar la salvaguarda de los intereses tanto individuales como colectivos respecto de la recolección, tratamiento y uso de la información de carácter personal.

Dentro de este orden de ideas, la ruptura epistémica que se produce consiste en la necesidad de lograr una eficacia material en torno a los mecanismos instaurados en la legislación en el campo de la protección de datos personales con la finalidad de evitar la vulneración de este derecho fundamental que les asiste a los usuarios de las entidades privadas. Los investigadores estudiados no analizan la problemática ni sus posibles soluciones desde la dimensión internacional, ni hacen referencia a lograr la efectividad de los mecanismos ya existentes en la legislación nacional en torno a la protección de datos personales por medio de una figura adaptada desde un ordenamiento jurídico ajeno al colombiano como una posible solución.

Por consiguiente, con la ruptura epistémica, queda formulada la pregunta problema de investigación de la siguiente manera: ¿Cómo se puede lograr la materialización de la legislación referente a la protección de datos personales para evitar la vulneración de los derechos de los usuarios de las entidades privadas?

Análisis de los mecanismos de control y vigilancia

A fin de llevar a cabo el establecimiento de un marco teórico capaz de encauzar y dirigir la conceptualización de la respuesta al interrogante de investigación es menester proceder a la sistematización de las claves teóricas y de la brecha metodológica que serán expuestas en este aparte.

Delgado Aguilar (2019), a través de su investigación establece que el modelo paternalista imperante en Europa para la protección de datos personales comprende la totalidad de los

elementos del procesamiento de los mismos considerando la protección de datos como un derecho de carácter fundamental y que la fijación de entes de control independientes constituye una garantía en torno a la correcta ejecución de la legislación sobre protección de datos; además, de ser menester que para aquellos datos personales que puedan exponer a sus dueños a situaciones de discriminación o vulnerabilidad por relacionarse de manera estrecha con el eje fundamental del derecho a la intimidad exista una protección especial por parte del Estado. Delgado Aguilar, resalta, además, que la adopción de una solución de este tipo por parte del Estado colombiano sería posible siempre y cuando exista confianza en las instituciones y una presencia sólida de la Superintendencia de Industria y Comercio. Desde otra mirada, el mismo autor hace referencia a una tendencia tecnológica, en la que las tecnologías se relacionan cada vez más de manera directa con el mayor uso y tratamiento de datos que caen dentro de la categoría de los datos personales, siendo necesario considerarlas como un elemento fundamental para la protección de los mismos (Delgado Aguilar, 2019).

Por la misma línea, encontramos autores como Rosario Serra Cristóbal, quien señala que "(…) deben ser, principios como los de consentimiento, necesidad, calidad, finalidad, información y seguridad, los que direccionen en la práctica, cuándo se pueden recopilar datos, cuándo pueden cederse, o qué medidas de seguridad se adoptan para evitar el acceso de terceros (…)". Además de considerar indispensable que ciertas actividades como recoger, manipular y exponer información personal y datos extraídos de comunicaciones se produzca únicamente en el evento de ser absolutamente indispensable para proteger la seguridad, sin que la misma pueda convertirse en una excusa para llevar a cabo ciertas actuaciones que resulten en la vulneración de derechos y libertades. Esta autora, precisa también, que en la práctica ciertas actividades que podrían transgredir el derecho a la protección de datos personales y otros afines, requieren mayor control,

pues son atendidas por el poder judicial y político únicamente a cierto nivel de penetración, sea esta cualitativa o cuantitativa (Serra Cristóbal,2015).

Andrés José González Porras (2016), considera que la serie de poderes y facultades de control que contempla el constitucional y legalmente reconocido derecho a la protección de datos personales recae en cabeza de los dueños de dicha información y que, por regla general, debería comprender las labores de formulación y utilización de los datos. Por otra parte, González Porras manifiesta respecto de otros asuntos asociados con la tutela de los datos personales que, actualmente, se evidencia un despliegue de actividades de varios entes a través del cual pueden llevar a cabo el monitoreo, recogida, análisis, uso, preservación u obtención de información contenida en las comunicaciones de los individuos, actividades que definitivamente no se han controlado adecuadamente y ha facilitado la posibilidad de comisión de actos irregulares y por consiguiente, la violación de los derechos de las personas. Por otra parte, este autor resalta que "(…) debemos adecuarnos a un nuevo ambiente global de información que ha puesto en entredicho el concepto tradicional de intimidad, para dar paso a nuevos matices conceptuales, a nuevas perspectivas de comunicación entre las personas y los países, generando con ello nuevos retos para el derecho a la protección de datos" (González Porras, 2016).

La vigilancia de los mecanismos que deberían proteger los datos personales de todos los habitantes del país debe realizarse, de manera armónica, con todo el apoyo institucional, además de las garantías y protección a este derecho fundamental. Siendo así, la protección de datos personales, para las prácticas profesionales del Derecho, supone entender estos como una estipulación de carácter constitucional y/o fundamental, enmarcado en el principio de seguridad. Asimismo, es indispensable resaltar que la exposición arbitraria de los datos personales puede

derivarse en una transgresión a este bien jurídico tutelado por el Estado, además de vulnerar otros derechos como la intimidad personal, el buen nombre y la honra.

La brecha consistirá entonces en inmiscuir el principio de seguridad en las prácticas profesionales del Derecho a través de la implantación de una figura utilizada por un referente más garantista en torno a la protección de los datos personales. Por el mismo camino, la viabilidad de la aplicación de dicha figura en el ordenamiento jurídico colombiano será validada a través de criterios de expertos e instituciones recopilados a lo largo del desarrollo de la presente investigación.

Capítulo II

El ordenamiento jurídico colombiano posee disposiciones tanto de carácter constitucional como de carácter legal y jurisprudencial orientadas a regular la recolección, tratamiento y uso de datos personales que llevan cabo las organizaciones públicas y privadas, siendo principalmente las actividades de recolección, tratamiento y uso ejercidas por estas últimas las que atañen a la presente investigación. En ese orden de ideas, encontramos que en la Constitución Política en su artículo 15, se señala que a todos los individuos les asiste el derecho a conocer, rectificar y actualizar la información recolectada respecto de ellos en bases de datos y en los archivos que manejan tanto entidades públicas como privadas, además de disponer que la recolección, tratamiento y circulación de datos deberá ser respetuosa de todas las garantías relacionadas al derecho de Habeas Data y demás derechos fundamentales en concordancia con este; por este mismo sendero, la Ley 1581 de 2012 objeto de reglamentación parcial por parte del decreto 1377 de 2013, desarrolla el derecho constitucional antes referido a través de principios y disposiciones por medio de los cuales se establecen los derechos de los titulares de los datos de carácter personal y las condiciones de legalidad para el tratamiento de datos.

Ahora bien, pese a la existencia de preceptos normativos que regulan la materia y contemplan mecanismos de protección, la eficacia de los mismos es precaria, pues el Estado se ha quedado corto a la hora de garantizar la materialización de lo dispuesto en la norma, derivando en la desprotección imperante de los derechos e intereses de los titulares de la información.

Para llevar a cabo el desarrollo de la presente investigación de tipo sociojurídico, que responde a un enfoque funcionalista y posee un alcance descriptivo, se optó por implementar el análisis de distintos ordenamientos jurídicos con la finalidad de realizar la recolección de alternativas en torno a la prevención y protección de los datos personales que han sido adoptadas por diferentes países en el mundo. Para lograr lo anterior, se realizó una observación investigativa

comparada frente a ordenamientos jurídicos ajenos a Colombia, haciendo énfasis en la Unión Europea y Norteamérica; así mismo, para recolectar y procesar los datos e información, se parte de la protección de datos personales como núcleo de análisis de las siguientes categorías a saber: i) perspectiva nacional de la protección de datos personales; ii) regulación internacional en materia de protección de datos personales; iii) mecanismos Internacionales para la protección de datos personales; iv) vertiente estadounidense y vertiente europea, ¿cuál es la mejor para Colombia? Y; v) mecanismo: Delegado de Protección de Datos -DPD-, una visión garantista para la prevención en materia de protección de datos en Colombia.

Prevención, preservación y protección de los datos personales: un análisis desde la perspectiva nacional e internacional

Perspectiva nacional de la protección de datos personales

En Colombia, en materia legislativa y jurisprudencial, se ha regulado hasta cierto punto en relación a los mecanismos para la salvaguarda del derecho fundamental establecido en el artículo 15 de la Carta Política que reza:

> Todas las personas (...) tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los 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, en relación al derecho de Habeas Data (Constitución Política de Colombia, 1991, Artículo 15).

Por otra parte, siguiendo a Garrigues (2018), encontramos *prima facie* la Ley 1581 de 2012 y el Decreto 1377 de 2013 que establecen la manera en que deben ser salvaguardados los derechos

de los titulares de los datos personales, así como las obligaciones en cabeza de quienes ejercen la recolección y tratamiento de los mismos. De manera previa, en el año 2008 fue expedida la Ley 1266 que se encargó de regular de manera específica la protección de datos personales en torno a la información de carácter crediticio y financiero y, adicionalmente, fue expedido el Decreto 886 de 2014 que reguló lo relacionado con el Registro Nacional de Bases de Datos, consistente en un directorio de carácter público de información alimentada por quienes realizan la recolección de datos personales; sin embargo, se considera que en materia legislativa sobre la protección de datos personales en Colombia, son la Ley 1581 de 2012 y el Decreto 1377 de 2013 los de mayor relevancia normativa.

En cuanto a la Ley 1581 de 2012, encontramos que esta posee un mayor alcance dado que su campo de aplicación se extiende a todas la bases de datos de Colombia, a la vez que complementa lo establecido en la Ley 1266 de 2008 en cuanto a los principios rectores, haciendo referencia a que el tratamiento de los datos personales puede efectuarse únicamente si se cuenta con el consentimiento previo, expreso e informado del titular de la información y que los mismos no podrán ser recolectados ni divulgados sin la autorización previa, además de hacer alusión a los datos sensibles 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. (Ley 1581, 2012, Artículo 5)

Además de precisar que respecto de los datos personales sensibles se prohíbe llevar a cabo su tratamiento, excepto cuando el titular lo autorice expresamente.

Se debe exaltar que, como considera Mantilla Valera (2019), tratándose de aquellos datos considerados como sensibles el titular de los mismos puede dar su autorización para el manejo de su información, lo cual no comportaría dificultad alguna si quienes otorgan su consentimiento lo hicieran de manera libre e informada, es decir, que los operadores brinden autorizaciones, ya sea físicas o digitales que sean lo suficientemente discriminadas en su formato de manera tal que el titular tenga la posibilidad de ejercer plenamente su derecho a suministrar únicamente una u otra información, pero en la práctica dichos formatos tienden a ser genéricos y limitarse a respuestas afirmativas y negativas, lo cual obstaculiza el margen de discrecionalidad a lo permitido.

Por otro lado, esta norma -Ley 1581 de 2012- establece también diversas medidas de control y seguridad que han de tenerse en cuenta respecto de la recolección y tratamiento de los datos personales de los titulares, como se observará a continuación en el siguiente cuadro:

Cuadro No. 02

Medidas de seguridad y control contempladas en la Ley 1581 de 2012

Ley 1581 de 2012	Medidas de control
Veracidad o calidad	Monitoreo de la información recolectada (completa, exacta, actualizable).
Finalidad	Aviso de Privacidad
Acceso y circulación restringida	Medidas y controles tecnológicos y físicos.
Seguridad	Medidas y controles tecnológicos y físicos.
Confidencialidad	Acuerdos de confidencialidad.
Transparencia	Procedimiento para cumplir el ejercicio de los derechos de los Titulares.
Legalidad	Política para la protección de datos personales
Libertad	Aviso de Privacidad / Autorización expresa del titular.

Fuente: Adaptado de *Medidas de Seguridad,* por Certicámara, 2021, Bibliotecadigital (https://bit.ly/2usbu5c)

Se observa que, en concordancia con los principios rectores que orientan el tratamiento de los datos personales a las luces de la Ley 1581 de 2021, encontramos diversas medidas de control y seguridad mediante las cuales se busca tutelar el derecho a la protección de datos personales en cuestión.

Ahora, tratándose del Decreto 1377 de 2013, este trae a colación otros conceptos sumamente relevantes en relación a los datos electrónicos, tales como la incorporación del aviso de privacidad, a través del cual se comunica la existencia de las políticas de tratamiento de la información aplicables, así como la manera en que se puede acceder a ella y lo relacionado con las finalidades del tratamiento que se les dará a los datos de carácter personal que sean recolectados. La misma norma señala qué aspectos deberá contener el aviso de privacidad en relación a la

necesidad y obligatoriedad de brindar información del tratamiento de los datos y su finalidad, además del carácter facultativo tratándose de datos sensibles (Mantilla De Valera, 2019).

Por otra parte, en materia jurisprudencial, el concepto de datos personales en Colombia se pudo entender por medio de la jurisprudencia de la Corte Constitucional a través del concepto de autodeterminación informativa. En ese orden de ideas, encontramos la sentencia T-414 de 1992, la cual hizo referencia a:

> Un nuevo poder de dominio social sobre el individuo, el denominado poder informático (…) la facultad de disponer de la información, de preservar la propia identidad informática, es decir, de permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás. (Corte Constitucional, Sentencia No. T-414, 1992)

En lo atinente a la noción de propiedad sobre los datos, la misma sentencia señaló que dada la complejidad de su naturaleza, frente a los datos no se puede aplicar en estricto rigor el clásico derecho de propiedad y que, dadas tales condiciones, los sujetos pueden considerarse como titulares de solo ciertas facultades, las cuales no les proporcionan necesariamente calidad de propietarios, sino que normalmente serán "simples depositarios forzosos". (Corte Constitucional, Sentencia No. T-414, 1992)

Por otra parte, la sentencia SU-082 de 1995 en armonía con el artículo 15 de la Carta Política aborda el tema referente al derecho del habeas data, relacionándolo con el derecho a la intimidad y al buen nombre, teniendo por resultado la incorporación del derecho al habeas data como un derecho inherente a la información privada de las personas. Por el mismo entramado, se

encuentra la sentencia C-446 de 1998, donde se recalca y reafirma la relevancia del derecho a la intimidad en el habeas data, en consonancia con el artículo 15 del Estatuto Constitucional.

Con base en lo anterior, se sientan los inicios del posterior criterio jurisprudencial, donde ciñéndose a los lineamientos de la Sentencia C-748 de 2011, actualmente se debe interpretar el habeas data como una garantía en torno al derecho a la intimidad, dando por entendido que los datos involucran tanto la vida privada como la familiar, por lo que ni el Estado, ni terceros pueden intervenir arbitrariamente. De igual manera, el reconocimiento de este derecho fundamental que goza de autonomía implica entender que el sujeto sobre el cual recae el derecho goza de "una cláusula de libertad, la cual le otorga facultades sobre la administración de su información" (Corte Constitucional, Sentencia No C – 748, 2011).

Por otra parte, se ha entendido en un inicio, que únicamente las personas naturales son sujetos de derechos y obligaciones, sin embargo, y en concordancia con lo expresado por Martínez (2019), a la luz del habeas data el derecho de la protección de datos personales se entiende, como: "un derecho fundamental autónomo que busca equilibrar las condiciones entre el sujeto de quien se informa y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo" (Corte Constitucional, Sentencia No T-1085, 2001). Por lo tanto, en su momento fue necesario que la jurisprudencia condicionara la aplicación del habeas data, ya que solo era reconocido para los seres humano y para las personas jurídicas no, por tal motivo se les reconoció a las personas jurídicas el derecho al buen nombre específicamente en la Sentencia T – 396 de 1993, lo que produjo que con posterioridad la Corte se pronunciara al respecto en su Sentencia T – 462 de 1997, la cual ha expresado que: "Las personas jurídicas son titulares del derecho fundamental al buen nombre, en consecuencia, lo son también del derecho al habeas data, toda vez que este último

derecho, reconocido por el artículo 15 de la Carta Política, existe justamente como garantía de aquel y del derecho a la intimidad personal y familiar" (Corte Constitucional, Sentencia T – 462,1997).

En ese mismo sentido y en aras de dejar en firme lo expuesto anteriormente, la Sentencia C – 748 de 2011 exalta y reafirma el hecho de que las personas jurídicas podrán hacer uso del derecho al habeas data ya que estas son conformadas por personas naturales y el derecho de estas mismas se extiende a sus sociedades.

Así pues, en Colombia, la Carta Magna establece que el tratamiento de los datos personales se encuentra tutelado por medio del derecho al habeas data, el cual es desarrollado con posterioridad a través de la Ley 1266 de 2008 y la Ley 1581 de 2012 reglamentada parcialmente por el Decreto 1377 de 2013. Por su parte, la jurisprudencia colombiana, "aborda la protección de datos personales como un derecho subjetivo complejo con garantía constitucional" (Corte Constitucional, Sentencia C-748, 2011).

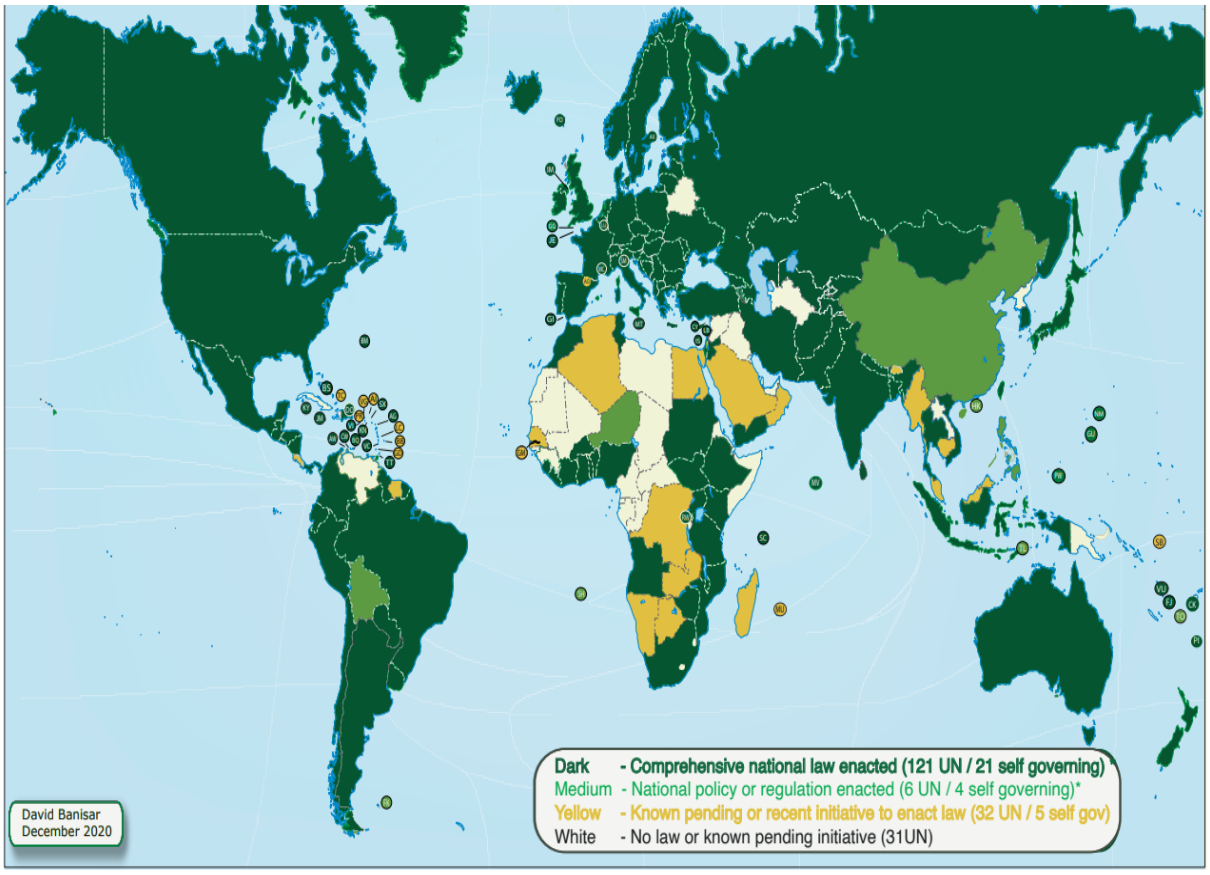
Regulación internacional en materia de protección de datos personales

Actualmente, el derecho fundamental a la protección de datos personales se encuentra reconocido, además de garantizado y protegido, tanto en el ámbito nacional, como en el contexto comunitario e internacional; siendo la responsabilidad el eje central de la mayoría de legislaciones que se involucran en el tratamiento de los datos personales y la protección de los mismos. Para Privacy International (2021), ONG del Reino Unido dedicada a llevar a cabo la vigilancia de las injerencias en la privacidad ejercidas por Estados y organizaciones, debe existir un ente regulador encargado de la implementación efectiva de las normas relacionadas con la protección de datos personales y la dimensión de las potestades conferidas a este tipo de entes o autoridades, así como su autonomía

o independencia del gobierno, varía de un país a otro. Asimismo, Banisar (2020) precisó que hasta diciembre de 2020 más de 120 naciones a nivel mundial han emitido leyes integrales de protección de datos con la finalidad de salvaguardar aquellos datos personales cuya custodia está en cabeza de entes de carácter público y privado.

Gráfica No. 02

Leyes, reglamentos e iniciativas sobre el derecho a la información (2020)



[1]

Fuente: Adaptado de *National Right to information laws Regulations and iniciatives 2020,* por Banisar David, 2020, SSRN: (https://ssrn.com/abstract=1857498)

[1] Nota: La ilustración representa la situación actual de los países del mundo en cuanto a la regulación en materia de datos personales.

Como es evidente, gran parte de los países en el mundo han venido expidiendo leyes integrales sobre protección de datos -países representados en color verde oscuro- o por lo menos cuentan con alguna regulación a nivel nacional en la materia -países representados en color verde medio- o en su defecto, tienen iniciativas pendientes para hacerlo -países representados en color amarillo-; actualmente son pocas las naciones que no han adelantado esfuerzos para legislar en relación a este tema -países representados en color blanco-, la mayoría de ellas pertenecientes al continente africano.

Hoy por hoy, se considera que es Europa el continente en el cual la protección de datos personales ha alcanzado mayor nivel; asimismo, se considera a Norteamérica como una región en la cual la protección de datos personales -principalmente en lo relacionado con el derecho a la privacidad- ha logrado un elevado nivel de desarrollo (Rodríguez, 2018). Sin embargo, ambos modelos, el europeo y el norteamericano, constituyen dos vertientes principales muy distintas la una de la otra en relación a la salvaguarda de información de índole personal; pues, por una parte, el modelo predominante en Europa tiene como finalidad salvaguardar tanto la información como su propiedad en pro de preservar el honor del individuo incluso cuando el mismo haya fallecido, basándose en los derechos humanos.

Por otra parte, Carlos G. (2004) señaló que el modelo norteamericano busca amparar la información de los sujetos a través del concepto del derecho a la privacidad, pero este perece con el fallecimiento de la persona y este modelo se fundamenta en relación a motivos meramente comerciales debido a que, por lo general, una vez fallece la persona las empresas pueden hacer uso de su información; sin embargo, no se discute su amplio nivel de progreso.

Cabe resaltar que el caso de Estados Unidos es único en el mundo porque, según Stranieri (2019), no cuenta con un conjunto legislativo unificado en relación a la privacidad de los datos,

sin embargo, ha acordado unos estándares mínimos de privacidad, en concordancia con lo establecido por la APEC -Asociación de Asia y el Pacífico-. Siguiendo el mismo lazo, la APEC es una organización que cuenta con Japón, Estados Unidos, Corea del Sur, México y Canadá entre sus 21 países miembros y a través de Las Reglas de Privacidad Transfronterizas estableció la base para las leyes relacionadas con la privacidad al interior de sus países miembros y las pautas de privacidad de datos establecidas son aplicables a todas las organizaciones de carácter público o privado que efectuen el tratamiento de datos personales. Las Reglas de Privacidad Transfronterizas se diferencian del RGPD imperante en la Unión Europea, entre otras cosas, en que fue creado únicamente con la finalidad de proporcionar mínimos niveles de protección y se aplica sólo a los controladores de datos, mientras que el RGPD se aplica tanto a controladores como a procesadores de datos.

Continuando con el panorama norteamericano en el campo de la protección de datos personales, se encuentra la Ley de Privacidad del Consumidor de California -CCPA- la cual ha sido inspirada en el GDPR de la Unión Europea, entró en vigor en 2020 y estipuló que las organizaciones privadas están obligadas a proteger los datos e información de carácter personal que logren obtener sobre los consumidores en California y abarca aspectos tales como, las políticas de privacidad, protecciones de seguridad y derechos del consumidor, entre los cuales se encuentran: conocer todos los datos que se recopilan y por qué, rechazar la venta de su información, solicitar la eliminación de sus datos y saber cuándo se comparten sus datos con terceros.

En el caso de Europa, como máximo referente en lo relacionado a la protección de datos personales; tiene lugar un avance sumamente importante en el campo legislativo sobre protección de datos personales con la adopción del Reglamento General de Protección de Datos de la Unión

Europea -RGPD-, el cual entró en vigencia en 2018, este reglamento integral comprende la mayoría de los tipos de tratamiento de datos personales y tiene efectos "no solo sobre quienes sean responsables de llevar a cabo el tratamiento de datos con base en la Unión Europea, sino también sobre todos aquellos que ofrezcan bienes o servicios a personas con base en la Unión Europea, así como sobre quienes realicen el seguimiento del comportamiento de dichas personas" (Privacy international, 2018).

Por el mismo entramado del RGPD, se observa que este instrumento abarca varios puntos clave que permiten incrementar las garantías cuya adopción debe ir de la mano con las medidas de protección pertinentes, los aspectos más importantes que incorpora son: i) la ampliación del catálogo de datos sensibles, incluyendo lo relacionado con la información genética y los datos biométricos; ii) la obligación de notificar a las entidades de control las brechas de seguridad que puedan perjudicar a los titulares y; iii) la obligación de los Responsables y Encargados del tratamiento, quienes deberán tomar las precauciones pertinentes con la finalidad de garantizar el cumplimiento de las disposiciones sobre protección de datos y se resalta la importancia de que las autoridades de supervisión, además de erigirse como entes sancionadores, inviertan en formación y concientización en la materia (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 2016, art.14).

Por otra parte, el Reglamento General de Protección de Datos que, al ser una norma a nivel de la Unión Europea, se aplica a países como Alemania, Austria, República Checa, Bulgaria Francia y España, entre muchos otros; como a las organizaciones con sede fuera de la Unión Europea que traten datos personales de los residentes en la UE, se acoge a lo establecido por la Comisión Europea (2012), que considera como datos personales de un individuo: nombres, fotos,

dirección de correo electrónico, detalles bancarios e incluso publicaciones en redes sociales, entre otros.

Cabe señalar también que, en virtud del RGPD se busca que las entidades retornen el control de los datos personales al individuo o titular, facilitando el acceso a aquellas organizaciones que llevan a cabo el tratamiento y permitiendo que tengan la posibilidad de cambiar los permisos que conceden para que los datos sean utilizados o compartidos.

El RGPD contempla, además, que cuando el tratamiento en el sector privado sea realizado por un controlador -organización que recolecta datos de residentes de la UE- cuyas principales actividades se basen en la ejecución de operaciones de tratamiento de datos personales que conlleven a la regulación y supervisión sistemática de los interesados, debe intervenir una persona experta en las leyes y las prácticas de protección de datos que estará encargada de ayudar al controlador o procesador a supervisar que se lleve a cabo el cumplimiento interno del reglamento y que se denominará Delegado de Protección de Datos.

Según el Reglamento General de Protección de Datos de la Unión Europea, el controlador de datos, además de tener la finalidad de demostrar el cumplimiento de dicho reglamento, debe poner en práctica medidas que vayan acorde a los principios de protección de datos por *diseño*, que, por su parte:

> Son medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 2016, art.25).

Y de protección de datos por *defecto*, que: "establece que deben de aplicarse medidas técnicas y organizativas apropiadas con el objeto de que se realice los tratamientos de datos realmente necesarios para los fines del tratamiento" (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 2016, art.25). Se requiere, además, que las medidas de protección de datos personales que se apliquen estén diseñadas para desarrollar procesos comerciales para productos y servicios. Por otra parte, el reglamento en su consideración No. 74 estipuló también que es responsabilidad del controlador de datos llevar a cabo la aplicación de medidas que sean oportunas y eficaces y que deberá ser capaz de demostrar que las actividades de tratamiento se han llevado a cabo de acuerdo con el reglamento.

En concordancia con lo anterior, la Agencia Española de Protección de Datos (2020) en un avance de su balance de cumplimiento correspondiente al año 2020, el cual reflejó que en menos de 2 años alcanzó un alto grado de ejecución en todos los ejes; señaló que su iniciativa más destacada durante el año 2020 consistió en aquella en virtud de la cual se pretendió valorar la privacidad como un activo que las entidades deben tener presente al momento de diseñar tanto sus políticas, como sus estrategias; siendo esto una muestra evidente de enfoque preventivo y responsabilidad proactiva del mismo modo que lo establece el Reglamento General de Protección de Datos vigente. Por el mismo entramado, indicó que no es suficiente con cumplir estrictamente con la legislación, sino que se debe ir más allá, de tal forma que a través de una actitud proactiva sea posible prevenir la comisión de futuras infracciones a la vez que se promueve una cultura en torno a la protección de los datos personales que son tratados y gestionados por los responsables o encargados, especialmente aquellos del sector privado.

Por todo lo anterior es claro que, a nivel de la Unión Europea, el Reglamento General sobre Protección de Datos -RGPD- provee un marco renovado y actualizado que se fundamenta en la rendición de cuentas en lo relacionado al tratamiento de datos personales para la protección de los mismos en Europa, a la vez que el Delegado de Protección de Datos -DPD- constituye el eje primordial de dicho marco jurídico para las entidades, pues facilita la materialización de los preceptos y disposiciones contenidos en el RGPD (Grupo de Trabajo Sobre Protección de Datos del Artículo 29, 2016). Asimismo, podemos afirmar que, como es evidente, gran parte de los países en el mundo han venido adelantando esfuerzos en torno al adecuado tratamiento de los datos personales, adaptando sus legislaciones a sus condiciones políticas, económicas y culturales.

Mecanismos a nivel de la Unión Europea para la protección de datos personales

En este aparte, se hará referencia a los mecanismos de control cuya aplicación se circunscribe exclusivamente al continente europeo dada la relevancia de sus aportes a la protección de datos personales y por tratarse de la región más destacada en cuanto a evolución normativa en dicho tópico.

En primer lugar, Cerda Silva (2006) expresa que hay que entender el control como determinada actividad que se acciona e implementa con la finalidad de comprobar, fiscalizar o inspeccionar el desempeño tanto propio como ajeno, que se establece no solo como algo necesario en un sistema jurídico si no como algo indispensable dentro del mismo; para que exista control se debe contar con dos parámetros muy importantes: el primero de ellos es la existencia de un marco normativo vigente y determinado, que debe ser conocido por parte del agente de control y por quien es objeto de su actividad; el segundo de ellos es la propuesta y adecuación de la conducta

que tiene que ser realizada por el agente de control, adecuando la actividad de quien es objeto de juicio conforme al marco normativo en cuestión.

Como ya lo antepone Cerda Silva, nos encontramos frente a una gran variedad de mecanismos de control previstos en Europa, los mismos, dada su relevancia para la presente investigación, serán descritos a continuación:

a) Control jurisdiccional: en primera instancia se encuentra el control jurisdiccional y de manera precisa el uso del habeas data, pero antes de abordar el tema es necesario realizar una distinción necesaria en la cual las normas referentes a la protección de datos invisten de competencia al orden jurisdiccional, haciendo un especial énfasis a los tribunales de justicia.

Se denota como factor común, que las disposiciones normativas otorgan a las autoridades nacionales de control ciertas facultades para así lograr la realización de sus fines, lo anterior sin suponer un requerimiento judicial previo; ejemplificándose de la siguiente manera:

> Disponer una medida cautelar respecto de sistemas de tratamiento de información, conferir o denegar la autorización para procesar determinada categoría de datos, oponerse al registro de cierta información suministrada por el responsable de tratamiento, o dictaminar la implementación de medidas de seguridad determinadas. (Cerda, 2006)

Por otra parte, es notable que las mismas leyes de protección de datos personales otorgan a los entes de control ciertas competencias, respecto de las cuales, para su ejercicio es necesaria una resolución judicial y un previo requerimiento.

Por consiguiente, según considera Cerda Silva, lo establecido en las legislaciones de protección de datos personales sobre la intervención judicial, no se limita al accionar del titular de

datos cuando este sufre un detrimento en su realidad jurídica ocasionado por el responsable del tratamiento, sino que además también ampara a este último en las reclamaciones que formule en contra de los pronunciamientos del ente de control, como también en las actuaciones entabladas por esta en contra de aquél.

En este orden de ideas, los Estados miembros dejaran por sentado que cada persona pueda disponer de un recurso judicial en el caso de ser violados sus derechos, lo anterior teniendo en cuenta el marco normativo vigente del estado miembro, con la finalidad de realizar la respectiva adecuación de la conducta, todo esto independientemente de los recursos administrativos que puedan entablarse ante la autoridad de control.

Por consiguiente, se puede afirmar que la totalidad de estados miembros en sus legislaciones admiten el control jurisdiccional frente a la protección y tratamiento de datos personales, aclarando que quien inicia o acciona este mecanismo es la persona que se vio afectada en el manejo, uso o tratamiento de sus datos personales; pero se ve viva la necesidad de encontrar un proceso más concentrado, específico y de tramitación simplificada, mediante el cual se otorgue una respuesta más oportuna, por lo cual surgió el reconocido habeas data. Consecuente a lo anterior, el término habeas data debe reconocerse en un ámbito más amplio, no solo refiriéndose a un proceso concentrado donde el titular de derecho hace efectiva la garantía del mismo, si no como aquel desglose procesal en el cual el afectado hace uso de su derecho de acceso, desde el momento que hace el requerimiento respecto de sus datos, pasando también por una reclamación administrativa hasta llegar a la mismísima acción judicial.

b) Códigos deontológicos: nacen por la necesidad de contar con disposiciones especiales referentes a la protección de datos, estos en su mayoría son expedidos por lo Estados miembros de

la Unión Europea y dentro de sus enfoques están inmersos los campos de evaluación crediticia, ámbitos laborales y los referentes a los fines de la seguridad social. Las disposiciones especiales se transforman en normativa específica, tal es el caso del tratamiento de datos en comunicaciones electrónicas, por otra parte, se crean y se especifican modelos orientadores por las autoridades de control nacional, todo lo anterior con la finalidad de combatir la obsolescencia de la norma y futuros procesos legislativos.

Según lo expresado por Cerda Silva, citando a Orti Vallejo (1994), los códigos deontológicos son aquellos cimientos jurídicos que resultan ser normas de conductas relacionadas con el tratamiento y almacenamiento de datos que por resultado terminan siendo adoptadas por determinados sectores gremiales, empresariales y profesionales. Por lo tanto, dichos códigos resultan ser para los agentes encargados del tratamiento y almacenamiento de datos una expresión de autorregulación, recalcando que en la elaboración y en el fomento de estos siempre está presente la participación de la autoridad pública con la finalidad de verificar la legalidad del mismo.

En el mismo sentido, la Directiva 95/46/CE del Parlamento Europeo y el Consejo de la Unión Europea (1995) hace un especial énfasis en los códigos de conducta en su capítulo V, expresando que cada uno de los Estados miembros de la Unión Europea y según sus competencias respectivas, deberán de manera oportuna alentar a la elaboración de los códigos de conducta con la finalidad de contribuir a la protección de datos en cada sector en específico, todo esto acompañado de un control judicial respectivo por la organización encargada.

c) Delegado de protección de datos: esta es la persona encargada y asignada para garantizar el cumplimiento de la normativa vigente referente a la protección de datos en la respectiva organización, empresa o gremio. En cuanto a las funciones del DPD estas se pueden

encontrar en el artículo 39 del RGDP. A continuación, se mencionan algunas de las más importantes:

> "informar y asesorar a todos aquellos que se ocupen del tratamiento de datos, supervisar el cumplimiento de lo dispuesto en la legislación europea en materia de protección de datos personales, ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación y, por último, cooperar con las autoridades de control y actuar como punto de contacto con las mismas" (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 2016, art. 39).

En pocas palabras el DPD es el encargado de velar por los derechos de las personas a las cuales se les trata o almacena los datos personales.

d) Autoridades de control: en cuanto a estas la Directiva es flexible respecto de su implementación, ya que cada una de ellas debe estar adecuada a la realidad jurídica e institucional del Estado miembro, sin embargo, la Directiva establece que todas las autoridades de control deben gozar de autonomía e independencia, en el entendido de que estas son necesarias para disponer de un máximo acatamiento de la norma.

Ahora bien, en lo que respecta a las funciones de estas autoridades de control encontramos las siguientes de manera general: i) por una parte le asisten funciones de difusión, asistencia y promoción en cuanto a la normativa vigente; ii) también encontramos la función de registro de entidades que tratan y almacenan datos personales; iii) otra función que reviste gran importancia es la de inspección, ya que con esta se podrá garantizar la protección óptima y adecuada de los sujetos de derechos que someten sus datos a tratamiento y almacenamiento. En ese orden de ideas no puede faltar la facultad sancionatoria ni mucho menos las facultades cautelares, toda vez que

por medio de estas se obtiene un castigo a quien infringe la norma y se previene la vulneración futura de derechos.

Vertiente estadounidense y vertiente europea ¿cuál es la mejor para el ordenamiento jurídico colombiano?

En primer lugar, se debe tener en cuenta que tal como lo señala la Sentencia C- 748/11, en el mundo imperan dos modelos de protección de datos: el modelo centralizado implementado en Europa – y el modelo sectorizado - implementado en Estados Unidos -, el primero de ellos orientado a la adopción de estándares generales y especiales aplicables tanto al sector público como al privado y el segundo, que no se basa en una categoría común de datos personales y por lo tanto no contempla que la totalidad de los datos deban someterse a una misma regulación (Corte Constitucional, Sentencia No C-748, 2011).

Según Carlos G., es menester señalar que, en el caso de Norteamérica, el derecho a la privacidad fue concebido a través de varias decisiones adoptadas por la Corte Suprema de Justicia en virtud de las cuales se reconoce que el Estado no puede inmiscuirse en las decisiones correspondientes a la esfera personal del individuo, por lo que se relaciona con la libertad dentro de un ámbito íntimo. El desarrollo del derecho a la privacidad en Norteamérica se fundamentó en un principio en la jurisprudencia y no fue sino hasta los años 70’ cuando comenzó su construcción normativa, enfocada en la preocupación de los individuos estadounidenses en cuanto a los abusos y excesivas demandas del mercado por lo que se caracterizó también por ser de carácter sectorial y fragmentado.

En el caso Europeo, por otra parte, la construcción de este derecho gira alrededor de la experiencia histórica ligada a la persecución secundada por la posibilidad de disponer de los datos

personales, pues se considera que anteriormente las bases de datos fueron utilizadas por los regímenes autoritarios para perseguir y exterminar por razones étnicas, raciales o políticas a millones de personas; por lo que en Europa se ha producido una conciencia pública en pro de la protección de los datos personales y aunque en principio cada país buscó legislar a su manera en materia de protección de datos, posteriormente se esforzaron en legislar de forma unificada basándose en un criterio más proteccionista.

Por otra parte, Carlos G. considera que, en Estados Unidos, el desarrollo jurisprudencial en relación al derecho a la privacidad se fundamenta en salvaguardar los sentimientos y sensibilidad de los ciudadanos y no sus intereses de carácter económico, por lo que se ha venido manteniendo la idea de que es un derecho de carácter personal que se extingue con la muerte de su titular. En contraposición a dicho fundamento, el sistema continental europeo sostiene que los derechos relacionados a la privacidad y a la intimidad están estrechamente enlazados al honor, por lo que aún fallecida la persona dichos derechos siguen siendo tutelados por entenderse que la memoria del fallecido constituye una prolongación de los derechos de la personalidad.

Además, mientras que en Europa se busca proteger a las personas a través de normas uniformes y de carácter general donde se estipule de manera específica los límites tanto del sector público como del sector privado para efectuar el tratamiento de los datos personales; en Estados Unidos las normas tienden a ser de carácter sectorial y se prefiere a menudo la revisión judicial de actos tendientes a agredir el derecho a la privacidad como aliciente para llevar a cabo la auto regulación.

En el caso Colombiano, la Sentencia C-748 de 2011 señala que el modelo de regulación adoptado en Colombia es un modelo híbrido donde convergen normas de carácter general con

normas de carácter sectorial, sin embargo, de todo lo anterior podemos concluir que el modelo de protección de datos personales que mejor se ajusta a la realidad de los países latinoamericanos como Colombia es el acogido por el sistema continental europeo, por ser de carácter más uniforme y proteccionista con tendencia a ser de índole preventivo, pues Europa se sirve de sus leyes para practicar mayores controles sobre el comportamiento de las grandes empresas y garantizar la protección de los datos personales de sus ciudadanos. Sin embargo, bajo el entendido de que un cambio de modelo per se, implicaría llevar a cabo un proceso sumamente complejo, Colombia podría optar por incorporar, cuando menos, uno o más de los mecanismos europeos en el campo de la protección de datos personales.

Mecanismo: Delegado de Protección de Datos -DPD-, una visión garantista para la prevención en materia de protección de datos

En relación con el Delegado de Protección de Datos o DPD, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (2016), indica que se debe iniciar señalando que éste consiste en una figura a través de la cual el Reglamento de Protección de Datos de la Unión Europea pretende lograr una mayor efectividad en lo relacionado a la protección de los datos personales de los individuos. Asimismo, se trata de una persona competente en los procesos relacionados con seguridad de datos, incluso en lo relacionado con el tratamiento de ciberataques, además de otras problemáticas relacionadas con la retención y el tratamiento de datos de carácter personal y confidencial.

El cúmulo de cualidades y experticia que se requieren de un DPD van más allá de la comprensión de las normas y disposiciones en torno a la protección de datos, además, el titular de dicho cargo constituye su correspondiente grupo de soporte, además de ser el encargado de su

propio y continuo crecimiento y desarrollo profesional. Además, el Delegado de Protección de datos debe ser un sujeto totalmente independiente de la entidad que lo emplea, por lo que actuará como una especie de regulador al interior de cada entidad que deberá garantizar que se lleve a cabo el cumplimiento del RGPD en lo atinente al tratamiento de datos personales que la misma lleve a cabo.

De conformidad con el RGPD, el Grupo de Trabajo Sobre Protección de Datos del Artículo 29 (2016) expresa que es obligatorio que parte de los encargados y responsables de ejecutar el tratamiento de datos personales, designen a un Delegado de Protección de Datos, sin embargo, inclusive en aquellos casos en los que el RGDP no precise de manera específica la designación de un DPD, las entidades de igual forma podrían considerar beneficioso o conveniente nombrar uno de forma voluntaria, pues para el Grupo de Trabajo del Artículo 29 "(…)que está conformado por un Representante de la Autoridad de Protección de Datos de cada estado miembro de la Unión Europea, el Supervisor Europeo de Protección de Datos y la Comisión Europea(…)" el DPD es el eje fundamental de la rendición de cuentas y su nombramiento facilita el cumplimiento del reglamento a través de la utilización de mecanismos para la rendición de cuentas, como las evaluaciones de impacto y auditorías de protección de datos, además, de comportar una ventaja competitiva para las empresas. Adicionalmente, los DPD proceden como intermediarios entre las partes interesadas, como podrían serlo las autoridades de control, las entidades y los usuarios de las mismas.

El Grupo de Trabajo Sobre Protección de Datos del Artículo 29, considera además que llevar a cabo el nombramiento de un Delegado de Protección de Datos es tan solo el primer paso, pues el mismo deberá tener, además, la autonomía y los recursos necesarios para desempeñar sus

funciones de manera efectiva; de forma tal que cumplidos dichos presupuestos, se reconoce al DPD como la piedra angular del sistema de gestión de datos.

Es menester señalar, además, que en materia de responsabilidad respecto del incumplimiento del RGPD, la misma recae sobre el encargado de realizar el tratamiento de los datos personales, pues es él quien es responsable de garantizar y demostrar que el tratamiento de los datos se ejecuta conforme a las disposiciones del Reglamento al mismo tiempo que juega un rol fundamental en lo relacionado a favorecer el desarrollo eficaz de las labores del Delegado de Protección de Datos, quien no será personalmente responsable por los incumplimientos del RGPD.

Por otra parte, Ramon Diaz (2019) haciendo mayor claridad sobre la naturaleza de la figura del DPD, cita al autor Simón Castellano, quien se refiere al mismo con el anglicismo "Data protection officer" señalando que este consiste en:

> Una figura nueva, creada por el legislador europeo mediante el RGPD (...) figura «independiente» que está en contacto permanente con el responsable del tratamiento, con terceros encargados de tratamientos, con los interesados o afectados por el mismo y con la autoridad pública de control (Ramon Diaz, 2019, p.8).

Sin embargo, el mismo autor recalca la definición señalada en el primer borrador del Reglamento General de Protección de Datos de la Unión Europea expedido en el mes de enero del año 2012, estableciendo que el DPD debe considerarse como "la persona responsable en el ámbito de la actividad del responsable o del encargado del tratamiento, para supervisar y monitorear de manera independiente la aplicación interna y el cumplimiento de las normas de protección de datos" (Ramon Diaz, 2019, p.8).

Asimismo, este autor hace referencia al criterio del autor López Calvo (2018), quien expresa que, no se debe pasar por alto que el Delegado de Protección de Datos deberá contar en todo momento con la confianza tanto a nivel profesional como ético del responsable o encargado del tratamiento de los datos personales, manteniendo su lealtad a este, tanto como su independencia; destacando que al no ser objeto de presiones por parte de los responsables y encargados antes mencionados se podrá afirmar que el DPD goza de todas las garantías para llevar a cabo su labor. Por el mismo camino, López Calvo afirma que en su concepto:

> El DPD es responsable de asegurar el cumplimiento del Reglamento y de la normativa nacional sobre la materia (…), de la formación y concienciación (de la plantilla y la dirección) del responsable/encargado que lo ha designado, con respecto a todos los tratamientos de datos personales realizados por este, siendo el punto de encuentro entre el responsable/encargado, los propietarios de los datos, su personal, los terceros que traten datos en su nombre y las autoridades de control. (López Calvo, 2018, p.496)

Lozano (2018) hace alusión a otro aspecto relevante en relación al RGPD y al DPD y es que estos permiten que las entidades adopten una cultura nueva a través de la cual ponen en primer lugar la privacidad, entendida como un activo importante para todo organismo, teniendo en cuenta que todos aquellos esfuerzos encaminados a salvaguardar los datos personales de sus usuarios y clientes influyen de manera positiva en su reputación como empresa a la vez que es útil a la hora de prevenir posibles sanciones que puedan tener lugar a causa de la inobservancia de lo establecido en el Reglamento. El mismo autor afirma que, la figura del DPD es una necesidad para el mercado actual, pues las empresas apuestan por la seguridad y confianza en dicha figura, por tratarse de una labor que desempeñan profesionales expertos y preparados en la materia, no sólo en cuanto a legislación, sino específicamente, en protección de datos personales.

En vista de todo lo anterior, es claro que el Delegado de Protección de datos constituye un factor decisivo del RGPD al actuar como garante de la observancia y respeto de la normatividad en torno a la protección de datos personales en las organizaciones, sin que ello implique una sustitución en las funciones ejercidas por las autoridades de control. (Agencia Española de Protección de Datos, 2018)

Aproximación a la tutela efectiva de los datos personales en Colombia

En este punto se brindará respuesta a la incógnita de investigación formulada en el capítulo primero, por consiguiente, se procederá a realizar una explicación exhaustiva de las aristas planteadas. Para llevar a cabo lo dicho, es menester tener en cuenta la pregunta de investigación, consistente en: ¿Cómo se puede lograr la materialización de la legislación referente a la protección de datos personales para evitar la vulneración de los derechos de los usuarios de las entidades privadas?

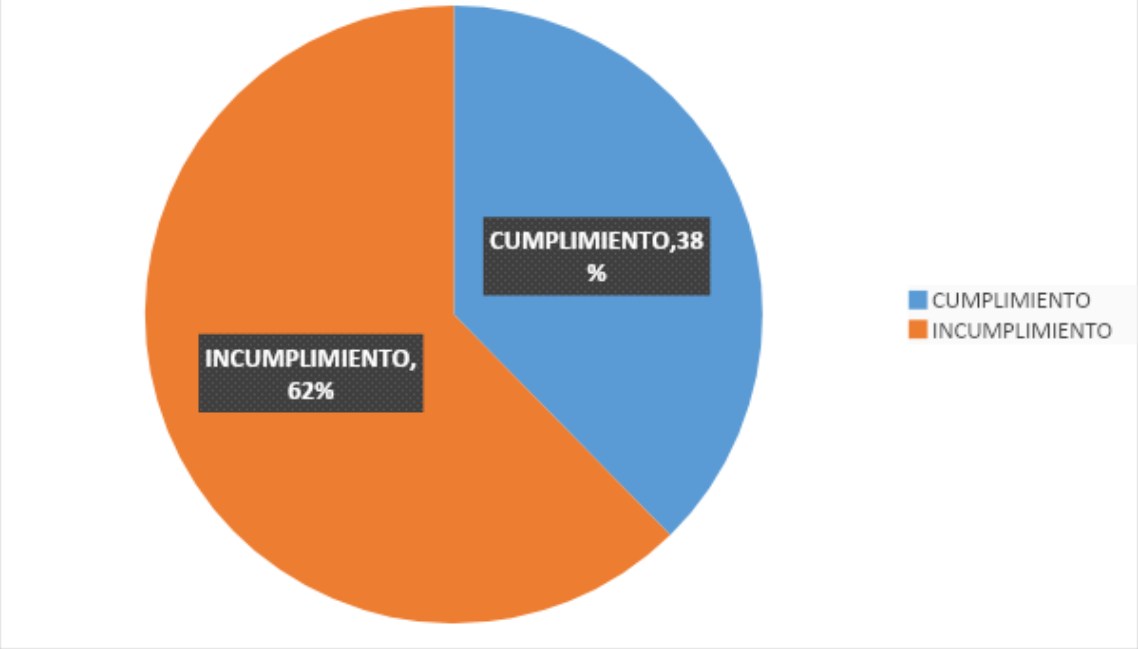
Los aspectos analizados con anterioridad, permiten vislumbrar que disposiciones normativas como el artículo 15 de la Constitución Política y normas posteriores como la Ley 1581 de 2012 y el Decreto 1377 de 2013, entre otras, han llevado a cabo el desarrollo del derecho fundamental y constitucional relativo a la protección de datos personales en torno a su recolección, tratamiento y uso por parte de las entidades de carácter privado.

Según la información recolectada en este capítulo y las cifras proporcionadas por la Superintendencia de Industria y Comercio por medio de la Delegatura para la protección de datos personales, se acredita que Colombia, pese a contar con legislación y mecanismos tendientes a salvaguardar el derecho a la protección de datos personales presenta un alto nivel de ineficacia

normativa, toda vez que no se cumplen las medidas pertinentes para la garantía del derecho en cuestión.

Gráfica No. 03

Promedio de observancia de medidas de protección en torno a los datos personales



Fuente: representación propia basada en las cifras proporcionadas por la SIC en su segundo estudio anual sobre medidas de seguridad. Información recuperada de: https://www.sic.gov.co/

Los datos recopilados por medio de la Superintendencia de Industria y Comercio, son la pieza clave para determinar el alto índice de incumplimiento en torno a las medidas de seguridad para la salvaguarda de los datos personales en Colombia, pues las cifras arrojadas no son satisfactorias. Se debe tener en cuenta que dichas cifras surgieron de la información suministrada por 33.596 entidades, de las cuales el 93.3% son privadas y se evaluaron ítems como: la implementación de medidas apropiadas y efectivas de seguridad, políticas de auditoría de

seguridad de la información, implementación de medidas especiales para proteger datos sensibles, entre otros.

Una vez expuesta la condición del derecho a la protección de los datos personales en Colombia, es menester poner de presente que este derecho también ha sido desarrollado en el ámbito internacional, encontrándose dos vertientes principales en la materia, como lo son la vertiente norteamericana y la vertiente europea, la primera de ellas centrada en salvaguardar la información de los individuos por medio de la conceptualización del derecho a la privacidad a través de la adopción de estándares básicos de protección de carácter general apoyados por leyes sectoriales y la segunda, es decir, la vertiente europea, enfocada en garantizar el derecho a la protección de los datos personales por medio del establecimiento de normas y reglamentos generales y uniformes que propenden por otorgar los más altos estándares de protección a través de múltiples mecanismos y herramientas.

Según los criterios recolectados, se han venido logrando altos niveles de garantía especialmente a nivel de la Unión Europea con la implementación del Reglamento General de Protección de Datos o RGPD como un esquema integral y renovado, cuyo efecto comprende la mayor parte de los tipos de tratamiento de datos personales y su aplicación se extiende más allá del tratamiento realizado con base en la UE, por otra parte, incorpora aspectos fundamentales como la obligación que recae sobre los responsables del tratamiento de asegurar que se acate la reglamentación en la materia, además de apostarle a la inversión en formación y concientización en este tema por parte de las autoridades de control, más allá de la simple imposición de sanciones.

Autoridades internacionales en el ámbito de la protección de datos personales, como la Agencia Española de Protección de Datos, concuerdan en que además de cumplir con la legislación se debe prevenir la comisión de futuras conductas violatorias del derecho y propender por una

cultura alrededor de la protección de datos personales, especialmente en relación a aquellos que son tratados en el sector privado.

Cabe destacar que, de acuerdo con la información recolectada, sin lugar a dudas la figura más preponderante en Europa en torno a la tutela efectiva del derecho a la protección de datos personales es la del Delegado de Protección de Datos o DPD, consistente en un mecanismo por medio del cual el RGPD de la Unión Europea busca una mayor eficacia en cuanto a la garantía del derecho en cuestión; dicha figura consiste en una persona experta en legislación en el campo de la protección de datos y procesos relacionados con la seguridad de los mismos, quien debe ser totalmente independiente de la entidad donde presta sus servicios y que opera como una especie de auditor-regulador al interior de cada entidad, garantizando que se dé cumplimiento a lo preceptuado en el Reglamento General de Protección de Datos en cuanto al tratamiento de los datos personales.

Según Rodríguez, M. (2018) la implementación de esta figura no es obligatoria para todas y cada una de las entidades, sin embargo, aquellas que no estén obligadas a adoptarla, también podrán hacerlo de forma voluntaria pues su designación facilita enormemente el cumplimiento de la norma, por lo que puede convertirse, incluso, en una ventaja competitiva, pues puede influir de manera positiva en su reputación como empresa a la vez que ayuda a prevenir la imposición de sanciones que puedan ser impuestas con ocasión de la inobservancia de lo plasmado en el Reglamento.

Por otra parte, el DPD actúa como un intermediario entre las entidades, las autoridades de control y los usuarios, por lo que no pretende en ningún momento sustituir las funciones de las autoridades de control, sino ser el punto de encuentro entre estas, los encargados o responsables del tratamiento -empresas- y los titulares de la información. Además, se advierte entonces que, a

través de una perspectiva comparada, el Estado colombiano debe optar por la implementación de mecanismos en torno a la protección de datos personales, que permitan garantizar la eficacia de la normatividad establecida para tales fines con respecto a la recolección, tratamiento y uso de información de índole personal llevados a cabo por las entidades de carácter privado. Esto último, siendo posible a través de la implantación de la figura del Delegado de Protección de Datos, como profesional experto en la materia, para que este a través de sus funciones como regulador independiente al interior de cada entidad favorezca la materialización de la normatividad vigente y de los mecanismos en ella establecidos, evitando así la transgresión del derecho fundamental a la protección de datos personales por parte de las entidades de índole privada.

Capítulo III

De acuerdo con lo precedido, se logró determinar que en el ordenamiento jurídico colombiano no son suficientes los mecanismos contemplados para la eficacia normativa en torno a la recolección, tratamiento y uso de los datos personales por parte de las entidades privadas, toda vez que aún es notable la transgresión del Derecho fundamental a la protección de datos personales, del Derecho a la intimidad, del Derecho de Habeas Data y demás derechos concordantes, ergo, los datos personales de quienes participan como usuarios en las actividades financieras, de consumo o administrativas y todas aquellas que involucren el tratamiento de datos siguen siendo vulnerados por las entidades antes referidas. Siendo así, el mecanismo denominado Delegado de Protección de Datos que ostenta la región europea es la condición sine qua non para resolver en gran medida la problemática en torno a los tratos arbitrarios o indebidos de la información de carácter personal, toda vez que va a coadyuvar para la protección eficaz de los Derechos inherentes a los datos personales.

En concordancia con la normatividad y los mecanismos que regulan en Colombia la protección de los datos personales en torno a su recolección tratamiento y uso, que se hallan señalados en la Constitución política, las Leyes, Decretos y Jurisprudencia, caracterizados por encaminarse a regular las actividades relacionadas al tratamiento de datos de índole personal, sin embargo, no han sido suficientes para salvaguardar de forma efectiva el derecho fundamental a la protección de datos personales. En virtud de lo anterior, las disposiciones jurídicas más relevantes en la materia, son: la Ley 1266 de 2008, conocida también como Ley de Habeas Data, la Ley 1581 de 2012, que fija las disposiciones de carácter general para la protección de datos personales y el Decreto 1377 de 2013, que reglamenta parcialmente dicha ley, entre otras. Por otra parte, a escala de la Unión Europea, se encuentra en el ámbito legislativo el Reglamento General de Protección

de Datos como medida primordial para la unificación legal y la garantía efectiva del derecho fundamental a la protección de datos.

La Ley 1266 de 2008, a través de su artículo 7, numeral 8, estableció como una de las obligaciones de los operadores de los bancos de datos, tramitar directamente las solicitudes, consultas o quejas a que haya lugar por parte de los titulares de la información. Por otra parte, en Europa, el numeral 4, del artículo 38 del Reglamento General de Protección de Datos, precisó que los titulares de la información pueden ponerse en contacto, en primer lugar, con el Delegado de Protección de Datos –DPD-, en lo relacionado al tratamiento de sus datos y el ejercicio de sus derechos.

De otro lado, la Ley 1581 de 2012, en su artículo 8, literal a, señala que el titular de la información personal tendrá derecho a la rectificación, conocimiento y actualización de sus datos personales frente a los Responsables o Encargados del tratamiento, de manera concordante con el artículo 15 de la Carta Magna, que hace referencia, además, al Derecho a la intimidad personal y familiar y al buen nombre a la vez que resalta que es deber del Estado respetarlos y hacerlos respetar. Haciendo referencia nuevamente a la Ley 1581 de 2012, la misma establece en el artículo 8, literal d, que es un derecho del titular de los datos personales presentar las respectivas quejas a la Superintendencia de Industria y Comercio - SIC - cuando se haya contravenido lo dispuesto en la ley; por su parte, la normativa europea en relación al DPD, indica como una de sus funciones en el artículo 39, literal d, la de colaborar con el ente de control, cuyo equivalente en el caso colombiano sería precisamente la SIC.

El Decreto 1377 de 2013, en su artículo 13, determina que son los mismos responsables del tratamiento quienes deben velar porque las políticas para el tratamiento de datos personales sean cumplidos por parte de los encargados del tratamiento; mientras que en el caso europeo, el

Reglamento General de Protección de Datos, en su artículo 39, literal b, en relación al Delegado de Protección de Datos, ha determinado que es este el encargado de garantizar la aplicación de las normas sobre protección de datos, incluidas las políticas para el tratamiento, al interior de las organizaciones.

De las normas nacionales mencionadas en el presente capítulo se puede inferir que, pese a que dichas disposiciones contemplan mecanismos tendientes a la protección de los datos de carácter personal, su alcance no logra un nivel de suficiencia adecuado para evitar la vulneración del derecho en cuestión a través de tratos indebidos o arbitrarios a la información de los titulares; pues el propósito de las mismas se encamina en lo relacionado al establecimiento de deberes en cabeza de los Responsables y Encargados del tratamiento así como de los derechos de los titulares, las condiciones de legalidad para llevar a cabo el tratamiento, además de procedimientos e instrumentos de control; sin embargo, en la realidad no se ven materializados dichos preceptos.

No obstante la existencia de estas disposiciones normativas, la recolección, tratamiento y uso de los datos personales se lleva a cabo de forma abusiva por parte de las entidades privadas, sin seguir los lineamientos establecidos legalmente para tales fines, lo que significa que no hay un mecanismo eficiente que garantice el cumplimiento de la norma y consecuentemente la tutela del derecho fundamental y constitucional a la protección de los datos personales, ocasionando que los derechos de los titulares de la información sean objeto de vulneraciones y abusos y generando a su vez el incumplimiento de los fines esenciales del Estado colombiano.

Es preciso, por lo tanto, que el Estado Colombiano implemente un mecanismo que permita lograr la eficacia material de la legislación vigente, siendo esto posible por medio la figura denominada Delegado de Protección de Datos, actualmente instaurada en los países miembros de la Unión Europea.

En cuanto al Delegado de Protección de Datos, su labor primordial consiste en actuar de forma independiente con la finalidad de garantizar que la normatividad se aplique de manera efectiva en la organización donde presta sus servicios, por lo que su implementación en el sistema jurídico colombiano puede ser de gran utilidad en miras a lograr la puesta en práctica de la regulación interna en torno a la protección de datos personales.

Asimismo, de acuerdo con el Reglamento General de Protección de Datos, artículo 39, numeral 1, el DPD se encarga de brindar información y asesoría completa sobre las obligaciones que les competen, tanto a los Responsables y Encargados del tratamiento de la información como a los empleados de la organización; esto podría coadyuvar en el sistema colombiano, a prevenir, desde el interior de las entidades la inobservancia de las normas y la consecuente violación de los derechos de los titulares de la información, esto último teniendo en cuenta que el logro de una tutela real a estos derechos depende en mayor parte de la adopción de medidas preventivas y no de medidas correctivas, como las que son aplicadas actualmente en Colombia por la SIC. (Mendoza, J. A., 2015)

Por otra parte, cabe resaltar que la figura del DPD, posibilita la configuración de una alternativa para la resolución amistosa de las controversias que pudieren tener lugar, pues el interesado tendrá la posibilidad de poner en conocimiento del mismo cualquier reclamación que no hubiese sido atendida en primer lugar por el Encargado o Responsable del tratamiento, antes de que dicha reclamación llegue a conocimiento de la autoridad de control (Ley Orgánica 3/2018, 2018), que en el caso colombiano sería la SIC, logrando así brindar una respuesta mucho más oportuna a los requerimientos de los usuarios en lo relacionado con el manejo que realice la entidad de sus datos personales, de esta manera lo han implementado países miembros de la UE como

España y para Colombia constituiría una figura novedosa, pues no existe actualmente un mecanismo similar en el ordenamiento jurídico nacional.

Sin duda, las facultades más significativas que le han sido atribuidas al Delegado de Protección de Datos en Europa, tal y como reza el literal b, del numeral 1 del artículo 39 del Reglamento General de Protección de Datos Personales, consisten en llevar a cabo la labor de:

> supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los 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 (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo , 2016, art. 39).

De lo anterior, se logra advertir que se trata de un mecanismo integral, que no se circunscribe a la imposición de medidas sancionatorias que traten la problemática una vez ya ha sido transgredido el derecho, sino que a través de labores de formación del recurso humano involucrado de manera directa en el tratamiento, de supervisión en cuanto al cumplimiento de todo el conjunto normativo en materia de protección de datos - desde las políticas del Responsable o Encargado al interior de la entidad, pasando por las demás disposiciones tanto a nivel de la UE como de cada Estado miembro, hasta el Reglamento General de la Unión Europea en el ámbito de la protección de datos personales – y de labores de auditoría interna, va encaminado a garantizar efectivamente desde un principio que los datos de índole personal sean recolectados o tratados por las entidades con observancia de las disposiciones regulatorias en el campo de la protección de los datos personales.

Considerando el desarrollo argumentativo esbozado con anterioridad, se logra advertir que Colombia no cuenta con mecanismos que propendan por garantizar de manera eficaz el cumplimiento de lo fijado en el ordenamiento jurídico como condición esencial para la salvaguarda efectiva de aquella información perteneciente a la esfera privada y personal del individuo, permitiendo así, que la misma sea objeto de manejos inadecuados y favoreciendo de igual forma la vulneración de un derecho fundamental reconocido en el ámbito nacional e internacional como lo es el derecho a la protección de los datos personales; para remediar la problemática expuesta, el Estado Colombiano debe implementar la figura del Delegado de Protección de Datos para a través de esta asegurar la observancia de las disposiciones instauradas en el marco legal vigente en relación a la salvaguarda de la información personal y el derecho en cuestión a fin de privilegiar la aplicación efectiva del principio de seguridad.

El DPD como la clave para la materialización del principio de seguridad y la subsecuente aplicación efectiva de los mecanismos en torno a la protección de los datos personales

La ley 1581 de 2012 contempla el principio de seguridad, en virtud del cual se estipula que aquella información que sea objeto de tratamiento, ya sea por parte del Responsable del Tratamiento o del Encargado del Tratamiento, deberá ser manejada teniendo en cuenta tanto las medidas técnicas como las medidas humanas e incluso aquellas de carácter administrativo que sean pertinentes con la finalidad de brindarle seguridad a los registros para evitar que la información contenida en los mismos sea adulterada, extraviada, consultada arbitrariamente o sea sometida a usos o accesos no autorizados o fraudulentos.

Por otra parte, la Sentencia C-478/11 señala que del principio de seguridad se desprende la responsabilidad en cabeza del administrador de los datos y declara además que la consolidación de dicha responsabilidad constituye actualmente un asunto de interés para la comunidad

internacional a causa del efecto denominado “diluvio de datos”, con arreglo al elevado volumen de datos de índole personal existentes que son sujetos a tratamientos y transferencias aumentan vertiginosamente y sin cese alguno.

La Corte precisa, además, que el avance de la tecnología ha provocado el incremento de los sistemas de información, los cuales hoy por hoy no reposan en simples bases de datos, toda vez que han emergido otros fenómenos, tales como las redes sociales, las prestaciones de servicios en línea y el comercio por medio de redes, además de muchos otros factores; lo que produce un aumento importante del riesgo de que se produzca una filtración de datos, por lo que se hace necesaria la incorporación de medidas que sean eficaces y permitan que dichos datos sean conservados, teniendo en cuenta que una manipulación indebida de la información podría acarrear perjuicios significativos, no meramente en lo relacionado al ámbito económico, sino también en relación al ámbito personal y el buen nombre.

La Sentencia referida hace hincapié en que, de conformidad con el principio de seguridad, tanto el Responsable como el Encargado del tratamiento, se encuentran en la obligación de ejecutar todas las medidas concordantes en relación al sistema de información que corresponda, de modo que, incluso tratándose de las redes sociales -que constituyen actualmente una fuente ampliamente utilizada para la recolección de datos por parte de organizaciones de todo tipo- se ha empezado a acrecentar el interés por instaurar mecanismos reforzados de protección relacionados al tratamiento de datos con carácter reservado.

A la luz de lo anterior, la Corte trae a colación lo expuesto por el Grupo de Trabajo Sobre Protección de Datos de la UE (2009) en relación a la importancia de salvaguardar los datos de los usuarios a través de la incorporación de “parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos”, pues a nivel de la Unión Europea, se

considera la seguridad como uno de los aspectos que necesariamente deben disponer de todas las garantías pertinentes en relación a la protección de datos personales, por lo que el Grupo de Trabajo estableció ciertos criterios en virtud de los cuales el acceso a los datos de índole personal debe ser objeto de protección, ya que de lo contrario, imperaría la desconfianza en el usuario en razón a la incertidumbre respecto de si su información será tratada o no de modo adecuado.

Por consiguiente, se evidencia la existencia de una obligación en cabeza de los Responsables y/o Encargados, consistente en el establecimiento de controles de seguridad con arreglo a la clase de datos objeto de tratamiento, a través del cual se posibilite la garantía de los estándares de protección incorporados en la norma.

Aguilar (2018) considera que al ser los datos personales un activo de carácter fundamental, un grupo de datos de índole personal proporcionan información importante perteneciente a la esfera privada e íntima de un individuo, atendiendo a este motivo y a la amplitud de información que los datos personales permiten obtener, es menester que estos gocen de una salvaguarda especial en lo relacionado a la manera en que estos circulan, son administrados, manipulados y tratados. De ahí que los estándares de seguridad deban ser muy altos y las políticas formuladas en el ámbito de protección deban brindar garantías suficientes en torno a la calidad de la información.

El mismo autor resalta que el principio de seguridad propende por la adopción de los mecanismos de protección necesarios y efectivos para desarrollar el proceso de tratamiento de datos personales, con la finalidad de atenuar el riesgo de pérdida de información, adulteración de los datos suministrados, desactualización y otros incidentes que pudieran presentarse y que conllevarían el riesgo de comprometer la seguridad de la información.

Por el mismo entramado, expresa Aguilar que ejercer el control necesario para que la información cuya administración se está ejerciendo disponga de total seguridad constituye una obligación para los Responsables y Encargados, quienes están en la obligación de adoptar técnicas especializadas en seguridad informática, además de planes de contingencia e identificación de riesgos y, básicamente, la totalidad de las medidas a que haya lugar con el objetivo de fijar un esquema de seguridad integral en el proceso de tratamiento de datos.

En consonancia con Aguilar, destacan Cuartas y Jaller (2014) que el principio de seguridad constituye una obligación que recae sobre los Encargados y Responsables del tratamiento de datos personales consistente en la adopción de mecanismos capaces de garantizar la seguridad en la administración de la información, en vista de que estos se relacionan con el ámbito privado de la persona y que muchos de esos datos deben ser objeto de una protección aún mayor atendiendo a su naturaleza, como puede ser el caso de los datos sensibles.

Será posible, entonces, privilegiar el principio de seguridad en el desarrollo práctico del Derecho para la solución a la problemática planteada a través de la adopción de una figura perteneciente a una legislación externa, pues como lo afirma Watson (1993) a través de la implementación de normas originarias de otras legislaciones el ordenamiento jurídico que rige una sociedad se transforma y evoluciona.

Por el mismo camino, López Medina (2015) señala que a través de la revisión de ordenamientos jurídicos extranjeros es posible construir la noción de mejores políticas públicas en determinada materia. Asimismo, Morales de Setién (2006) afirma que el acogimiento de normas pertenecientes a un ordenamiento jurídico ajeno constituye un mecanismo esencial de expansión de ideas de índole jurídico y la manera más relevante de trasformación jurídica y en concordancia

con Monateri (2006) quien sostiene que los ordenamientos jurídicos tienden a ser una combinación de modelos acogidos de otros ordenamientos.

Por otra parte, para Peña (2019), el principio de seguridad supone la salvaguarda de los datos en sí, constituyendo el enfoque principal sobre el cual se sustentan las diversas normativas de protección de datos personales que en consonancia con este principio propenden por el amparo o protección de la información con el objetivo de que la misma no sea objeto de posibles injerencias que pudieran causarle algún perjuicio a su titular.

Advierte el mismo autor, además, que dada la relevancia que ostenta la información personal para los titulares de los datos en relación a la salvaguarda de sus derechos fundamentales, el principio de seguridad comporta la necesidad de que el responsable proteja efectivamente los datos que se encuentren a su disposición, atendiendo a la obligatoriedad de que, tal y como lo afirma Peña citando a Jervis (2006) "se adopten medidas apropiadas para proteger los bancos de datos contra 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 informático" (Jervis, 2006, p. 65).

Garrido (2015) hace referencia a que el principio de seguridad, a manera de obligación sobre el Responsable del tratamiento, advierte que:

> "(…) seguridad se define como la serie de medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, cualquiera sea el método de tratamiento, particularmente a través de las redes de comunicación. Estas medidas deben aplicarse en niveles o en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse" (Garrido, 2015, p. 82-83).

Concluye Peña, que debe verse a la seguridad como un principio rector en la reglamentación de la protección de datos personales y que este constituye un imperativo para el responsable del tratamiento consistente en la tutela de los datos respecto de posibles intervenciones indebidas de los que estos puedan ser objeto, teniendo que incorporar mecanismos de control y seguridad tendientes a garantizar dicha salvaguarda. En ese orden de ideas, esta obligación se circunscribe, concretamente a la incorporación de mecanismos de protección de la información de índole personal en consideración a los efectos negativos que pudieran tener lugar ante la eventual vulneración.

El principio de seguridad que debe imperar en los procesos de recolección, tratamiento y uso de los datos personales llevados a cabo por las entidades privadas se verá beneficiado en las prácticas profesionales del Derecho con la implementación del Mecanismo del Delegado de Protección de Datos, a partir de fundamentos teóricos y legales de la perspectiva nacional e internacional, en razón al análisis de los modelos imperantes en la materia a nivel global y los mecanismos implementados en la Unión Europea como referente en el tema, para lograr la materialización efectiva de la legislación vigente en relación a la protección de datos personales, garantizando así el manejo seguro y adecuado de la información personal que suministran los usuarios a las entidades ya referidas, evitando que estas utilicen de manera indebida, ilegal o ilícita los datos del titular, perjudicándolo.

El Delegado de Protección de datos como mecanismo para la tutela efectiva de los datos personales de los usuarios de entidades privadas

Nelson Remolina, actual Superintendente Delegado para la Protección de Datos Personales, ha sido enfático al precisar que aún hay fallas en torno a la salvaguarda de la información personal de los individuos. En este sentido, señala lo siguiente respecto de los sistemas de información:

> "(…) se nutren de datos personales, ofrecen innumerables posibilidades para recolectar, almacenar y circular esa información en poco tiempo y de manera imperceptible para las personas a que se refieren los datos, no son absolutamente seguros, evolucionan rápidamente y traspasan las fronteras físicas" (Remolina, 2010, p. 492).

Las vulneraciones al derecho fundamental a la protección de datos personales obedecen a la inobservancia de los mecanismos establecidos en la ley en torno a la recolección, tratamiento y uso, toda vez que las entidades privadas no siguen el procedimiento adecuado para garantizar a los usuarios la plena y efectiva protección de sus datos personales.

Lo anterior constituye una problemática que vale la pena considerar, ya que como lo dispone Cano (2012), la ausencia de controles sobre la información que está sujeta a recolección y manejo por parte de las empresas, ya sea con o sin autorización de su titular, ha suscitado desconfianza entre los usuarios en torno a la manera en que dichas organizaciones gestionan sus datos personales.

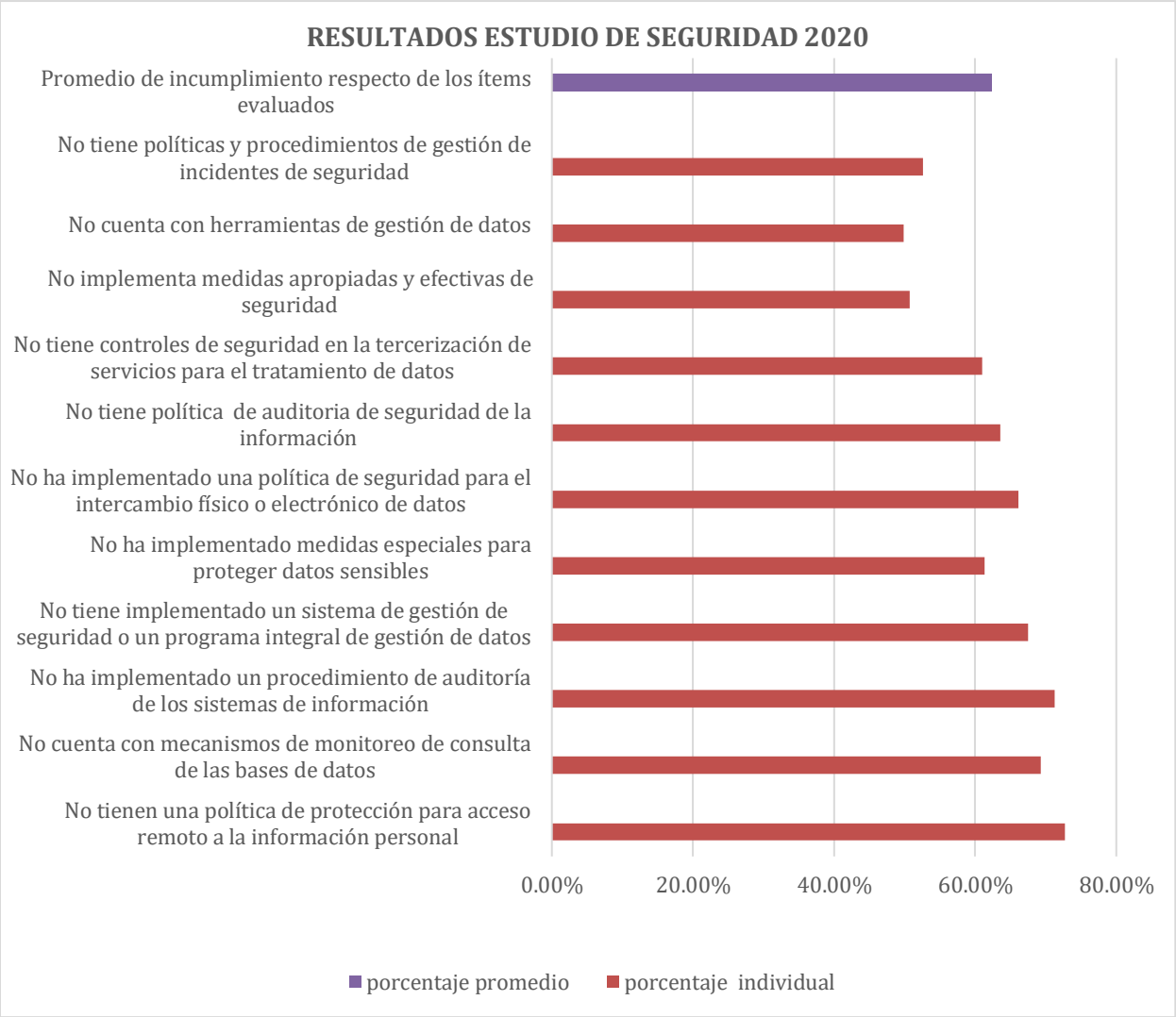
Mantilla Valera (2019) expone que en cuanto al tratamiento de los datos personales catalogados como sensibles existe actualmente una dificultad relacionada con el consentimiento del titular de la información, toda vez que los operadores no proveen formatos de autorización lo suficientemente claros y discriminados que permitan el ejercicio pleno de los usuarios en torno a su derecho de suministrar los datos de acuerdo con los presupuestos de libertad e información establecidos en la ley, puesto que son muchas las organizaciones que ni siquiera solicitan

autorización del titular para recolectar este tipo de información y otras tantas organizaciones lo hacen utilizando simples formularios genéricos.

Para corroborar lo señalado por Mantilla Valera y otros expertos, basta con analizar la Gráfica No. 04, sobre las cifras presentadas por la Superintendencia de Industria y Comercio, como autoridad nacional en materia de protección de datos personales y como administrador del Registro Nacional de Bases de Datos en relación con la implementación de medidas de seguridad para la recolección, tratamiento, uso y circulación de datos personales; donde se evidencia que más del 50% de las organizaciones evaluadas no cuentan con medidas apropiadas y efectivas de seguridad, el 61,3% no implementó medidas especiales para la protección de datos sensibles, el 66,1% no ha llevado a cabo la implementación de políticas de seguridad para llevar a cabo el intercambio físico o electrónico de datos y más del 67% no ha implementado sistemas de gestión de seguridad ni programas integrales de gestión de datos, los porcentajes de incumplimiento en los demás ítems son igualmente desalentadores y de las organizaciones evaluadas, más del 90% corresponden a empresas del sector privado, siendo estas las que presentan mayores índices de inobservancia respecto de los mecanismos de seguridad contemplados en la ley.

Gráfica No. 04.

Resumen ejecutivo del estudio de seguridad correspondiente al año 2020



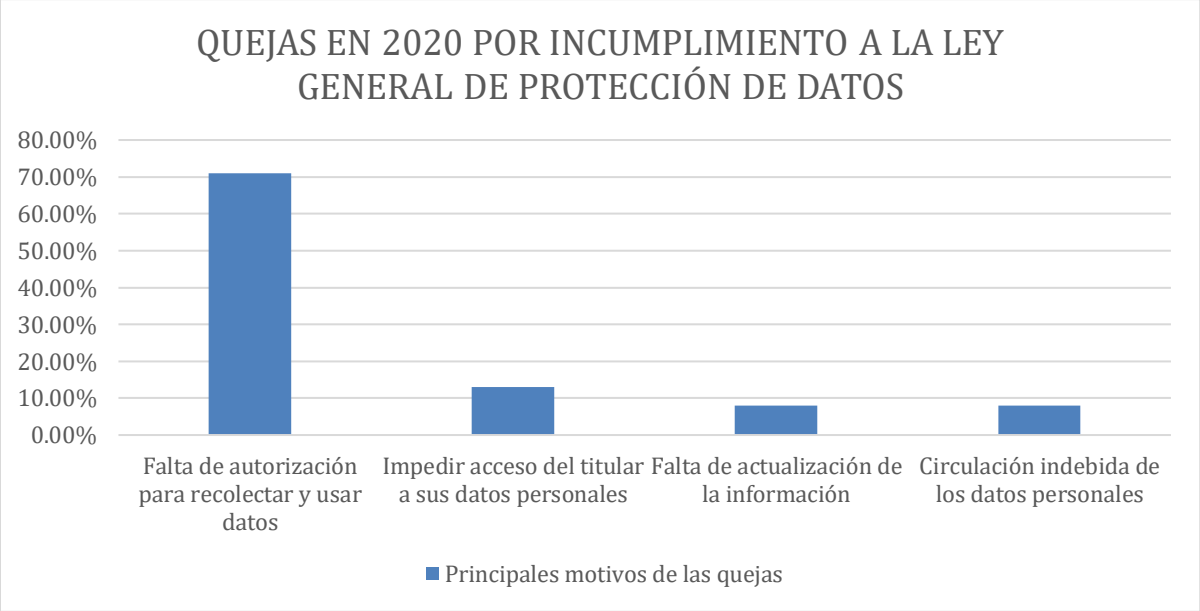
Fuente: Representación propia. Estudio de medidas de seguridad en el tratamiento de datos personales. Superintendencia de Industria y Comercio (2021).

Gonzales Porras (2016), manifestó que actualmente un sin número de organizaciones llevan a cabo actividades de monitoreo, recogida, análisis y uso de información de carácter personal sin que se aplique un control adecuado sobre las mismas, favoreciendo la comisión de conductas irregulares y, por ende, la violación del derecho a la protección de datos personales. A propósito de lo manifestado por Gonzales Porras, de acuerdo al Balance de Gestión emitido por la Superintendencia de Industria y Comercio correspondiente al año 2020, de las quejas recibidas por

incumplimiento a la Ley General de Protección de Datos, más del 70% están relacionadas con la carencia de autorización para llevar a cabo la recolección y uso de los datos, siendo la autorización del titular una de las medidas de control dispuestas en la ley 1581 de 2012 para amparar el derecho a la protección de datos personales.

Gráfica No. 05

Análisis de quejas recibidas en 2020 por la Superintendencia de Industria y Comercio por inobservancia de la Ley 1581 de 2012



Fuente: Representación propia. Superintendencia de Industria y Comercio (2021).

Como consecuencia de las constantes vulneraciones a la protección de datos personales, pese a ser un derecho constitucional y legalmente reconocido, a través de las cifras presentadas por la autoridad nacional en materia de protección de datos en sus estudios, balances y el criterio de expertos en la materia, se ha logrado evidenciar que es palpable la ineficacia de las disposiciones y mecanismos formulados para la protección de los datos personales en torno a su recolección,

tratamiento y uso, en especial, tratándose de aquellos datos pertenecientes a los usuarios de las entidades de carácter privado.

Ahora bien, una vez expuesto *grosso modo* el problema de eficacia que se advierte en relación a la materialización efectiva de los mecanismos de control en torno a la recolección, tratamiento y uso de los datos personales y la consecuente vulneración del derecho a la protección de datos personales como derecho fundamental, el Estado en virtud del artículo 15 de la Constitución Política, en consideración del principio de seguridad, debe incorporar la figura del Delegado de Protección de Datos -DPD- como instrumento que favorecerá la protección de los datos personales. En consonancia con la información recolectada, se evidencia que tanto organizaciones como expertos concuerdan en que el DPD es una figura que impulsa la aplicación material de las disposiciones normativas en el campo de la protección de los datos personales por su presencia al interior de cada organización como también el control y acompañamiento que ejerce de manera directa.

De acuerdo con Carlos G. (2004), es predominante en Europa la concepción de la protección de los datos personales como un derecho cuya salvaguarda es esencial a raíz de sus antecedentes históricos ligados a las consecuencias negativas de la disposición indiscriminada de la información de las personas por parte de los regímenes autoritarios, lo que ha llevado a la región Europea a adelantar esfuerzos de manera continua con miras a proteger los datos personales de sus ciudadanos, convirtiéndose en el principal referente a nivel mundial en la materia. En vista de lo anterior, sería beneficioso para Colombia replicar, legislativamente y atendiendo el contexto nacional, el empeño de los países europeos por salvaguardar el derecho en cuestión, concretamente, a través de la implementación de la figura del Delegado de Protección de Datos, inclinándose a la adquisición de una postura más garantista en este tema y entendiendo el derecho

fundamental a la protección de datos personales como una estipulación de carácter constitucional enmarcada en el principio de seguridad y el habeas data.

Por el mismo camino, Lozano (2018) resalta la funcionalidad preventiva del DPD, por su rol como formador y por su capacidad de prevenir la imposición de sanciones a los Encargados y/o Responsables del tratamiento de datos como resultado de la inobservancia de las normas que regulan lo concerniente al manejo de los datos, en el sentido de que al tratarse de una persona experta en el campo de la protección de datos personales que se encuentra en contacto permanente con los Responsables y Encargados del tratamiento puede direccionar su actividad, de modo tal que se eviten las vulneraciones a los derechos de los titulares de la información, verificando que se acaten las directrices legales para la recolección, tratamiento y uso de los datos personales; que en el caso colombiano, consistirían en llevar a cabo el monitoreo de la información, hacer uso de avisos de privacidad, solicitar el consentimiento expreso del titular, adoptar políticas internas para la protección de los datos personales, entre otras, que, como se ha demostrado, no se están aplicando de manera eficaz.

En consonancia con Lozano, afirma Mendoza (2015) que la consecución de una garantía efectiva en torno a los datos personales está sujeta en gran parte a la implementación de medidas encaminadas a **prevenir** las conductas vulneradoras a través de las cuales se lleva a cabo la manipulación arbitraria e indebida de los datos y no exclusivamente a la aplicación de medidas de carácter correctivo, en ese sentido, el DPD desarrollaría en Colombia un papel fundamental, pues su labor se orientaría, entre otras cosas, a asesorar permanentemente a los Responsables y Encargados sobre las obligaciones que les corresponden en relación al tratamiento de la información y actuar como una especie de regulador interno para garantizar el cumplimiento de las normas que rigen lo relativo al uso, tratamiento y recolección de datos de índole personal;

siendo necesario aclarar que esta figura no pretendería en ningún momento desplazar en sus funciones a la autoridad de control, pues como es evidente, en la práctica, la labor de esta última se inclina más a la recepción de quejas de los usuarios e imposición de sanciones y su campo de acción difícilmente se extendería al interior de cada entidad de forma directa y permanente como le correspondería hacerlo al Delegado de Protección de Datos.

De lo descrito a lo largo de la presente investigación, es posible determinar que la figura de origen europeo denominada Delegado de Protección de Datos, será vital para coadyuvar en la salvaguarda del derecho fundamental a la protección de datos personales habida cuenta de que facilitará la puesta en práctica de los mecanismos incorporados en la legislación colombiana para tal fin, contrarrestando el déficit de aplicabilidad de dichos mecanismos e impidiendo que las empresas incurran en actos tendientes a manipular indebidamente los datos de sus usuarios desconociendo las obligaciones que les asisten en virtud de la ley y vulnerando los derechos en cabeza de sus usuarios a través de conductas como rehusarse a implementar políticas especiales para la protección de datos sensibles, incumplir deberes específicos como solicitar la autorización respectiva para el tratamiento de los datos o informar al usuario sobre la finalidad del mismo, entre muchas otras.

Conclusiones

El Estado Colombiano ha consagrado constitucionalmente el derecho de Habeas Data a través del cual se desarrolla la protección de datos personales enmarcada en el principio de seguridad, a través del cual se busca que la recolección, tratamiento y uso de la información personal de los individuos se lleve a cabo teniendo en cuenta las medidas pertinentes para evitar que la misma sea objeto de manejos indebidos o arbitrarios. Sin embargo, actualmente existe una falla en relación a la tutela efectiva del derecho fundamental a la protección de datos personales, dado que las entidades privadas no cumplen con las directrices legales y constitucionales en torno a este derecho. En vista de lo anterior, el Estado debe implementar la figura del Delegado de Protección de Datos -DPD- a fin de garantizar la materialización de las disposiciones y por ende la salvaguarda del derecho.

De acuerdo con sus fines esenciales, el Estado Colombiano debe velar por la efectividad de los derechos contemplados en la Constitución. Por tal motivo, se debe privilegiar el principio de seguridad a través de la incorporación del Delegado de Protección de Datos en el ordenamiento jurídico colombiano, para que este contribuya a la materialización efectiva de los mecanismos y disposiciones contemplados en la ley para proteger a los usuarios de entidades privadas de injerencias indebidas y otras conductas relacionadas con su información que pudieran afectarlos en su órbita personal.

La necesidad de implantar la figura del DPD es cuando menos apremiante al constatarse que los mecanismos instaurados para la protección de los datos personales están siendo inaplicados por parte de los Encargados y/o Responsables del tratamiento de la información, lo que demuestra la ineficiencia de la legislación vigente en la materia, toda vez que en la práctica, los procesos de recolección, tratamiento y uso se llevan a cabo contrariando los deberes y exigencias legales, tales

como solicitar la autorización del titular para realizar el tratamiento, contar con un procedimiento especial para el tratamiento de los datos catalogados como sensibles, implementar medidas apropiadas y efectivas de seguridad, entre otros.

Para la efectividad normativa en torno a la protección de los datos personales, la implementación de instrumentos y mecanismos - como el DPD - debe considerar la existencia de altas cifras de incumplimiento por parte de las entidades privadas en torno a las medidas de seguridad encaminadas a proteger los datos de sus usuarios y los perjuicios que dicho incumplimiento acarrea para los titulares de la información no solo en relación a su derecho a la protección de los datos personales, sino a la protección de otros derechos afines como el derecho al libre desarrollo de la personalidad, al buen nombre, la intimidad y el honor, entre otros; toda vez que se evidencian dificultades a la hora de asegurar el respeto de principios y garantías constitucionales y legales con respecto al manejo de la información de carácter personal.

Con la presente investigación, se concluye que la figura del Delegado de Protección de Datos, está dirigida a lograr la materialización eficaz de las disposiciones y mecanismos establecidos en el ordenamiento jurídico colombiano para la protección de los datos personales como derecho fundamental inherente a los usuarios de las organizaciones de carácter privado, toda vez que se encargaría de orientar desde el interior de cada una de ellas la actividad de los Responsables y/o Encargados del tratamiento de conformidad con la ley.

Glosario

Aviso de privacidad: Es aquel comunicado verbal o escrito emitido por el Responsable del tratamiento de datos, dirigido al Titular de estos para el tratamiento respectivo de sus datos personales; por medio de este se informa acerca de políticas de Tratamiento de la información que le serán aplicables y además de esto las formas de acceder a las mismas y las finalidad es del tratamiento.

Autorización: Aquella acción realizada por el Titular encaminada en dar su consentimiento, previo, expreso e informado respecto del tratamiento de sus datos personales.

Base de Datos: Agrupación organizada de datos personales los cuales son objeto de Tratamiento.

Controladores de Datos: Es aquella entidad, persona, o autoridad pública encargada de decidir sobre los medios para procesar los datos personales y su finalidad.

Dato personal: Toda aquella información inherente a una o varias personas naturales determinas o determinables.

Datos sensibles: Son aquellos que, si se les da un uso indebido pueden afectar la intimidad del Titular ocasionando discriminación, tales como aquellos que revelen la orientación política, el origen racial o étnico, las preferencias religiosas, las orientaciones políticas, por otra parte, también se encuentran los datos relativos a la vida sexual, datos biométricos y salud.

Delegado de Protección de Datos: Persona experta y profesional en materia de protección de datos personales, que tiene como propósito el cumplimiento efectivo y material de las normas al respecto.

Empresa o Entidad Privada: Es una persona jurídica con ánimo de lucro, principal y exclusivamente constituida por particulares.

Encargado del Tratamiento: Es la persona responsable del tratamiento y por lo tanto es la encargada de realizar el mismo, esta actividad puede ser desarrollada por una persona natural o jurídica de carácter público o privado.

Procesadores de Datos: Es aquella entidad, persona, o autoridad pública encargada del procesamiento de datos personales en nombre del controlador.

Recolección: Es aquel acto por medio del cual se captan los datos personales del Titular.

Responsable del Tratamiento: Es la persona encargada de decidir sobre las bases de datos o el tratamiento de los mismos; esta persona puede ser natural o jurídica de carácter público o privado.

Titular: Cuya persona somete sus datos a tratamiento.

Transferencia: Es el proceso realizado por el Encargado o Responsable del Tratamiento de datos personales, en el cual este, teniendo por ubicación Colombia, envía a un receptor la información o datos personales, por lo cual, este también se convertiría en Responsable del Tratamiento.

Transmisión: es aquella comunicación de los datos personales que se realiza al interior o al exterior de un territorio, que tiene por finalidad el tratamiento por parte del encargado y a cuenta del responsable.

Tratamiento: Hace referencia a cualquier conjunto de operaciones realizadas sobre los datos personales, un ejemplo de ello es la supresión, uso, circulación, almacenamiento y recolección.

Uso Indebido: Aquella acción encaminada en dar mala utilización a los datos suministrados por el titular.

Referencias

Agencia Española de Protección de Datos. (01 de diciembre de 2018). *¿Qué es un Delegado de Protección de Datos?* Obtenido de Sitio WEB: https://www.aepd.es/es/prensa-y-comunicacion/blog/que-es-un-delegado-de-proteccion-de-dato

Agencia Española Protección Datos. (14 de septiembre de 2020). *Plan de Responsabilidad Social de la AEPD*. Obtenido de Archivo PDF: https://www.aepd.es/sites/default/files/2020-12/plan-responsabilidad-social-balance-2020-avance.pd

Aguilar Castañeda, M. A. (2018). La ley de protección de datos en Colombia: sus inicios y examen de sus principales postulados. Recuperado de: https://repository.ucatolica.edu.co/handle/10983/23060

Aliño, J. (2018). La protección del consumidor digital: los datos personales en el comercio electrónico. Revista Jurídica sobre Consumidores y Usuarios, numero, año (2018), pp. 97-115. Bogotá: Universidad Libre. Disponible en https://libros-revistas-derecho.vlex.es/, Consultado el 23 de abril de 2020.

Angarita, N. R. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?. International Law: Revista Colombiana de Derecho Internacional, 8(16).

Banisar, D. (1 de diciembre de 2020). *National Right to information laws, Regulations and iniciatives 2020* [Ilustración]. SSRN. https://ssrn.com/abstract=1857498

Becerra, M, Navarro, M. (2012). Retos actuales para la protección de datos personales en las organizaciones. Revista Jaiio, numero 41, año (2012), pp. 178-192. San Juan. Universidad Nacional de San Juan. Disponible en http://41jaiio.sadio.org.ar/. Consultado el 23 de abril de 2020.

Bejarano, M. R. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. Novum Jus: Revista Especializada en Sociología Jurídica y Política, 8(1), 107-139. Recuperado de: https://editorial.ucatolica.edu.co/

Cano, L. G. (2012). Protección de datos en Colombia, avances y retos. Revista Lebret, 4(4), 195-214. Recuperado de: http://revistas.ustabuca.edu.co/index.php/LEBRET/article/view/336

Carlos, G. (2004). Protección de Datos Personales: Europa vs. Estados Unidos, todo un Dilema para América Latina.

Cerda Silva, A. (2006). Mecanismos de control en la protección de datos en Europa. *Ius et Praxis, 12(2), 221-251. Recuperado de* https://scielo.conicyt.cl/scielo.php?pid=S0718-00122006000200009&script=sci_arttext&tlng=p

Certicámara. (2021). Medidas de Seguridad [Tabla]. Bibliotecadigital. https://bit.ly/2usbu5c

Colombia, Congreso de la República. Ley 1266 de 2008. (31 de diciembre de 2008). *Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones (consultado el 17 de abril de 2021). Recuperado de http://www.secretariasenado.gov.co*

Colombia, Congreso de la República. Ley 1273 de 2009. (05 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* (consultado el 17 de noviembre de 2019). Recuperado de http://www.secretariasenado.gov.co

Colombia, Congreso de la República. Ley 1581 de 2012. (18 de octubre de 2012). *Por la cual se dictan disposiciones generales para la protección de datos personales* (consultado el 17 de noviembre de 2019). Recuperado de http://www.secretariasenado.gov.co

Colombia, Consejo de Estado. (20 de abril de 2016). *Sentencia No 23001-23-33-000-2015-00506-01. [MP Sandra Lisset Ibarra Velez]* (consultado el 20 de noviembre de 2019) Recuperado de http://www.consejodeestado.gov.co

Colombia, Constitución Política. (07 de julio de 1991) Gaceta Constitucional No. 116 de 20 de julio de 1991 (consultado el 09 de abril de 2021) Recuperado de http://www.secretariasenado.gov.co

Colombia, Corte Constitucional. (06 de octubre de 2011). *Sentencia No C-748 de 2011 [MP Jorge Ignacio Pretelt Chaljub]* (consultado el 20 de noviembre de 2019) Recuperado de http://www.corteconstitucional.gov.co

Colombia, Corte Constitucional. (11 de octubre de 2001*). Sentencia No T-1085 de 2001 [MP Eduardo Montealegre Lynett.]* (consultado el 19 de abril de 2021). Recuperado de http://www.corteconstitucional.gov.co

Colombia, Corte Constitucional. (16 de junio de 1992). *Sentencia No T-414 de 1992 [MP Ciro Angarita Baron.]* (consultado el 19 de abril de 2021). Recuperado de http://www.corteconstitucional.gov.co

Colombia, Corte Constitucional. (24 de septiembre de 1997*). Sentencia No T-462 de 1997 [MP Vladimiro Naranjo Mesa]* (consultado el 17 de abril de 2021). Recuperado de http://www.corteconstitucional.gov.co

Colombia, Ministerio De Comercio, Industria y Turismo, Superintendencia De Industria Comercio. Decreto 1377 de 2013 (27 de junio de 2013). *Por el cual se reglamenta parcialmente la Ley 1581 de 2012* (consultado el 22 de septiembre de 2019). Recuperado de http://wsp.presidencia.gov.co/

Colombia, Ministerio De Comercio, Industria y Turismo, Superintendencia De Industria Comercio. Resolución 45743 de 2018 (29 de junio de 2018). Por la cual se impone una sanción y se imparten ordenes administrativas (consultado el 22 de septiembre de 2019). Recuperado de https://www.sic.gov.co/

Colombia, Ministerio De Comercio, Industria y Turismo, Superintendencia De Industria Comercio. Resolución 76434 de 2012 (04 de diciembre de 2012). *Por la cual se deroga el*

contenido del Título V de la Circular Única de la Superintendencia de Industria y Comercio, sobre Acreditación, y se imparten instrucciones relativas a la protección de datos personales, en particular, acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, las cuales se incorporan en el citado Título (consultado el 22 de septiembre de 2019). Recuperado de https://www.sic.gov.co/

Comisión Europea. (25 de enero de 2012). *La Comisión propone una reforma general de las normas de protección de datos para aumentar el control de los usuarios sobre sus propios datos y reducir los costes para las empresas*. Obtenido de Sitio WEB: https://ec.europa.eu/commission/presscorner/detail/es/IP_12_46

Cuartas Rodríguez, E., & Jaller Escudero, J. D. (2014). El Habeas Data como Derecho fundamental y la Ley 1581 de 2012 y su decreto 1377 de 2013 (Bachelor's thesis, Universidad EAFIT). Recuperado de https://repository.eafit.edu.co/

Del Estado, E. J. (2021). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Recuperado de http://travesia.mecd.es/portalnb/jspui/handle/10421/9132

Delgado Aguilar, F. (2019). *Comentarios a los sistemas de vídeo vigilancia en el marco del régimen de protección de datos personales* (Bachelor's thesis, Universidad EAFIT) (consultado el 22 de mayo de 2020). Recuperado de: https://patrimoniomusical.eafit.edu.co/

Delgado, L. R., & Pérez, M. M. S. (2010). Introducción a la protección de datos. Editorial Dykinson, SL. Recuperado de: https://books.google.es/

Directiva 95/46/CE del Parlamento Europeo y del Consejo. (24 de Octubre de 1995). Diario oficial de la Unión Europea. Unión Europea, Unión Europea: El Parlamento Europeo y El Consejo de la Unión Europea. Recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=ES

Galvis, L. (2012). Protección de datos en Colombia, avances y retos. Revista Lebret, número 4, año (2012), pp. 195-214. Bucaramanga: Universidad Santo Tomas. Disponible en http://revistas.ustabuca.edu.co/. Consultado el 23 de abril de 2020.

García, A. (2007). *La protección de datos personales: derecho fundamental del siglo xxi. un estudio comparado.* Revista Boletín Mexicano de Derecho Comparado, número 120, año (2007), pp. 743-778. Morelia: Universidad Latina de América. Disponible en http://www.scielo.org.mx/. Consultado el 23 de abril de 2020.

Garrigues. (2018). *¿Cómo se regula la protección de datos en Latinoamérica y cómo influye el RGPD?* Obtenido de Sitio WEB: https://www.garrigues.com/es_ES/noticia/regula-proteccion-datos-latinoamerica-influye-rgpd

González Porras, A. J. (2016). Privacidad en internet: los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva (consultado el 22 de mayo de 2020). Recuperado de: https://ruidera.uclm.es/

Grupo de Trabajo Sobre Protección de Datos del Articulo 29. (13 de diciembre de 2016). *Directrices sobre los delegados de protección de datos (DPD).* Obtenido de Archivo PDF: https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf

Herrán, A. (2002). El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales. Madrid: Dykinson. Disponible en https://books.google.es/. Consultado el 23 de abril de 2020.

Jervis Ortiz, P. (2006). La regulación del mercado de datos personales en Chile. Recuperado de: http://repositorio.uchile.cl/

López Calvo, J. (2018). El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid: BOSCH - Wilster Kluver.

López-Medina, D. (2015). El nacimiento del derecho comparado moderno como espacio geográfico y como disciplina: instrucciones básicas para su comprensión y uso desde América Latina. International Law: Revista Colombiana de Derecho Internacional, (26), 117-159. Recuperado de: https://www.redalyc.org/pdf/824/82442792004.pdf

Mantilla De Valera, L. C. (2019). Tratamiento de datos personales y las plataformas digitales reseña sobre Colombia y la Unión Europea. Recuperado de https://repository.javeriana.edu.co/bitstream/handle/10554/47067/TRABAJO%20DE%20GRADO%20VERSI%c3%93N%20FINAL%20LAURA%20MANTILLA%20%282%29.pdf?sequence=2&isAllowed=y

Martínez, A. (2019). La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales? Revista La Propiedad Inmaterial, numero 27, año (2019), pp. 5-23. Bogotá: Universidad Externado de Colombia. Disponible en https://dialnet.unirioja.es/. Consultado el 23 de abril de 2020.

Mendoza, J. (2015). Protección de datos personales en Colombia. Bogotá: Universidad Militar Nueva Granada. Disponible en https://repository.unimilitar.edu.co/. Consultado el 23 de abril de 2020.

Millanes, V. (2017). Desafíos en el debate de la protección de datos para Latinoamérica. Revista Transparencia y Sociedad, numero 5, año (2017), pp. 13-31. Chile: Consejo para la transparencia. Disponible en https://www.consejotransparencia.cl/. Consultado el 23 de abril de 2020.

Monateri, P. G., & Samuel, G. (2006). La invención del derecho privado (pp. 1-266). Siglo del Hombre Editores. Recuperado de: https://iris.unito.it/handle/2318/35270#.YII89OhKhPY

Morales de Setién Ravina, C. (2006). La invención del derecho privado. Colección Nuevo Pensamiento Jurídico, Siglo del Hombre Editores, Bogotá.

Ornelas, L, Higuera, M. (2013). La autorregulación en materia de protección de datos personales: la vía hacia una protección global. Revista de Derecho, comunicaciones y nuevas tecnologías, numero 9, pp. 5-30. Bogotá: Universidad de los Andes. Disponible en https://bibliotecausatpdqt.files.wordpress.com/. Consultado el 23 de abril de 2020.

Peña Yáñez, S. (2019). Régimen de indemnización de perjuicios de la Ley N° 19.628 y la seguridad de datos personales. Análisis crítico del principio de seguridad de datos del artículo 11° de la Ley de protección a la vida privada y su aplicación práctica. Recuperado de: http://repositorio.uchile.cl/handle/2250/175622

Privacyinternational.org. (31 de marzo de 2021). *Guía para Involucrarse en Políticas Públicas de Protección de Datos.* Obtenido de Archivo PDF: https://privacyinternational.org/sites/default/files/2018-11/Part%201%20-%20Proteccio%CC%81n%20de%20Datos_web_1.pdf

Ramon-Diaz, A. (2019). El Delegado de Protección de Datos en la Administración local (Master's thesis). Recuperado de: https://reunir.unir.net/bitstream/handle/123456789/8191/

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. (27 de abril de 2016). Diario Oficial de la Unión Europea. Unión Europea, Unión Europea: El Parlamento Europeo y el Consejo de la Unión Europea. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679.

Rodríguez, M. (19 de enero de 2018). *La protección de datos en el panorama internacional. Una primera aproximación*. Obtenido de Sitio WEB: https://dpd.aec.es/la-proteccion-datos-panorama-internacional-una-primera-aproximacion/

Rodríguez Villabona, A. A. (2016). La interacción entre ordenamientos jurídicos: trasplante, recepción, adaptación e influencia en el Derecho. IUSTA, 2(31). Recuperado de https://doi.org/10.15332/s1900-0448.2009.0031.07

Ruiz, B. (2016). Regulación en materia de protección de datos personales o habeas data en Colombia. Bogotá: Universidad Católica de Colombia. Disponible en https://repository.ucatolica.edu.co/. Consultado el 23 de abril de 2020.

Sánchez, C. (2009). La protección de datos personales de las personas vulnerables. . Revista Anuario de la facultad de Derecho, número 1, año (2009), pp. 203-227. Alcalá: Universidad de Alcalá II. Disponible en https://ebuah.uah.es/. Consultado el 2 de abril de 2020.

Scola, S. (2015). El tratamiento de datos personales y el resarcimiento de daños: desde la normativa europea hasta la solución adoptada en Italia. Revista R.E.D.S, numero 7, año (2015), pp. 146- 161. Verona: Università degli Studi di Verona. Disponible en: https://dialnet.unirioja.es/. Consultado el 23 de abril de 2020.

Serra Cristóbal, R. (2015). La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional. Revista de Derecho Político, 92, 73-118 (consultado el 22 de mayo de 2020). Recuperado de: http://e-spacio.uned.es/

Stranieri, S. (27 de septiembre de 2019). Leyes Globales De Privacidad De Datos: USA, UE, China Y Más. Obtenido de Sitio WEB: https://blog.ipswitch.com/es/leyes-globales-de-privacidad-de-datos-usa-ue-china-y-m%C3%A1s

Superintendencia de Industria y Comercio. (11 de marzo de 2021). *Más de 24 Mil Empresas No Tienen Mecanismos Eficientes Para Proteger Los Datos de Sus Usuarios de Accesos No Autorizados. Obtenido de Sitio WEB: https://www.sic.gov.co/slider/m%C3%A1s-de-24-mil-empresas-no-tienen-mecanismos-eficientes-para-proteger-los-datos-de-sus-usuarios-de-accesos-no-autorizados*

Superintendencia de Industria y Comercio. (28 de enero de 2021). *Más de 16 mil quejas recibió la Superindustria en 2020 por protección de datos personales. Obtenido de Sitio WEB: https://www.sic.gov.co/slider/m%C3%A1s-de-16-mil-quejas-recibi%C3%B3-la-superindustria-en-2020-por-protecci%C3%B3n-de-datos-personales*

Superintendencia de Industria y Comercio. (2021). *Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales.* Obtenido de Archivo PDF: https://www.sic.gov.co//sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

Watson, A. (1993). Legal Transplants: An Approach to Comparative Law (2ªedición obra original publicada en 1974). Georgia: University of Georgia Press.