EL HABEAS DATA COMO DERECHO FUNDAMENTAL Y LA LEY 1581 DE 2012 Y SU DECRETO 1377 DE 2013

ELISEO CUARTAS RODRÍGUEZ

JUAN DAVID JALLER ESCUDERO

UNIVERSIDAD EAFIT

ESCUELA DE DERECHO

MEDELLIN

2014

EL HABEAS DATA COMO DERECHO FUNDAMENTAL Y LA LEY 1581 DE 2012 Y SU DECRETO 1377 DE 2013

ELISEO CUARTAS RODRÍGUEZ

JUAN DAVID JALLER ESCUDERO

Trabajo de grado presentado para optar al título de Abogado

Asesor: Oscar Alberto Rodríguez Ortega
Director Jurídico de Fenalco Antioquia

UNIVERSIDAD EAFIT
ESCUELA DE DERECHO
MEDELLIN
2014

CONTENIDO

Pág.

INTRODUCCION

El mundo está en constante transformación, se presentan nuevos e innovadores cambios en las comunicaciones, en la salud, en la tecnología, entre otros. Con motivo de lo anterior, también se generan nuevas formas de vulnerar los derechos de las personas. Lo que hace necesario ampliar el contenido de los derechos fundamentales, y expedir normas y reglamentos para la protección de los mismos.

El presente trabajo, tiene como objeto principal resaltar la importancia de usar de manera correcta y con la mayor responsabilidad posible la información que se tiene de las personas, así como los derechos y obligaciones que se tienen entre sí los titulares de la información con la persona que los manipula. Además busca indicar qué derechos se involucran en la manipulación de datos personales, mostrar su núcleo esencial, y en general explicar aspectos importantes de la nueva Ley 1581 de 2012 y el decreto 1377 de 2013 que la reglamenta.

También se indicará como solucionar el conflicto entre dos derechos fundamentales a la hora de establecer una limitación al mismo por parte del legislador (principio de proporcionalidad) y cuando en un caso concreto se contraponen dos derechos (ponderación).

De tal suerte que con el presente trabajo se pretende establecer un mapa de conocimiento al lector, de tal forma que de manera general pueda saber qué derechos y obligaciones tiene como titular o como tratante de los datos de las personas a partir de la jurisprudencia y legislación vigente en Colombia.

1. JUSTIFICACIÓN

A lo largo de la historia se han presentado grandes avances tecnológicos y nuevos medios de comunicación; resulta evidente que la regulación de los mismos no se desarrolle a igual velocidad. La legislación en estos temas es de vital trascendencia e importancia, puesto que se pueden llegar a vulnerar derechos fundamentales de las personas tal como se manifiesta en la Sentencia T-414 de 1992 de la Corte Constitucional Colombiana en la que cita el "Proclama de Teherán" aprobada por la Conferencia Internacional de Derechos Humanos el 13 de Mayo de 1968 que reza: "*…Si bien los recientes descubrimientos científicos y adelantos tecnológicos han abierto amplias perspectivas para el progreso económico, social y cultural, esta evaluación puede, sin embargo, comprometer los derechos y las libertades de los individuos y por ello requerirá una atención permanente…".*

Así se refleja la preocupación que se tiene en este tema no sólo de manera actual, sino también desde tiempo atrás y de manera global. En la vida en sociedad, el manejo e intercambio de datos se ha convertido en una actividad habitual, tanto en el sector público como en el privado. Estos datos se utilizan para el desarrollo de las actividades diarias, como por ejemplo vender bienes (exigen determinada información, no sólo cuando el medio es el internet), prestar algún servicio (información para una cirugía, tomar determinado seguro, estudiar en algún lugar), o también inclusive en el ámbito laboral (exigen hoja de vida, llenar solicitudes, referencias personales, etc.). De tal manera que se hace necesaria la regulación de estas actividades en donde se relacionan datos personales de las personas.

En el caso Colombiano, la protección de los datos personales no es nueva, si bien el artículo 15 de la Constitución de 1991 reconoció por primera vez y explícitamente el derecho al habeas data, desde años atrás ya existía una preocupación en el Congreso y el Ejecutivo por proteger los datos personales.

Entre las iniciativas en la materia, vale la pena destacar la Ley 23 de 1981 *"Por la cual se dictan normas en materia de ética médica"*, cuyo artículo 34 dispone que la historia clínica *"[e]s un documento privado sometido a reserva que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley*", y la Ley 96 de 1985, cuyo artículo 51 reconoce la naturaleza pública de los datos sobre número de identificación personal y lugar y fecha de expedición, pero otorga carácter reservado a los archivos que reposan en la Registraduría ligados a la identificación, como datos biográficos, filiación y fórmula dactiloscópica.[1]

Frente al flagrante cambio que estaba teniendo el mundo a nivel tecnológico e informático nuestra Carta Constitucional dispuso en su Artículo 15 el derecho al Habeas Data, la intimidad y al buen nombre, pero la Carta Superior sólo enumera los derechos no los desarrolla por lo cual era necesaria una Ley Estatutaria para llenar de contenido y regular íntegramente dicho derecho al habeas data, tal como lo manifiesta la Corte Constitucional: *"…A partir de la vigencia del art. 15 de la Carta del 91 y en desarrollo del mismo es indispensable la regulación integral del poder informático para poner coto a sus crecientes abusos. Así lo exige la adecuada protección de la libertad personal frente a los poderosos embates de las nuevas tecnologías. Y así lo ordenará esta Sala".*[2]*.*

De tal manera que la Corte Constitucional era consciente de la necesidad de una Ley que tenga por objeto la regulación integral del poder informático. Así entonces sólo hasta el año 2008 con la Ley Estatutaria 1266 se logró regular parcialmente el tema, ya que el objeto de dicha Ley señala:

> …tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el

[1] CORTE CONSTITUCIONAL. Sentencia C-748 de 2011, p. 22
[2] Ibid, Sentencia T-414 de 1992, M.P. Ciro Angarita Barón , p. 18

> artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países... (Negrillas fuera de texto original).

A pesar que desde el año de 1992 la Corte Constitucional mostraba la necesidad de una regulación de datos e información de las personas, tal como se dijo anteriormente, nótese que el objeto de la Ley 1266 de 2008 habla de regular unos datos muy específicos, que son la información financiera y crediticia, comercial y de servicios. De tal manera, que no se estaría regulando íntegramente el poder informático, y quedan interrogantes como: qué pasa con aquellos datos que no tienen dicha naturaleza, qué regulación tienen las bases de datos de las empresas de información personal de sus empleados, qué pasa con los datos que piden las empresas que prestan el servicio al domicilio de las personas, en general qué pasa con todos aquellos datos que no son objeto de regulación de la Ley 1266 de 2008 y que sin embargo se recogen, se tratan, se usan y comercializan y que posiblemente con dicha actividad se vulneren los derechos de las personas, entre ellos el derecho a la intimidad, el habeas data, el buen nombre, información, entre otros, dependiendo de cada caso concreto. Así entonces el presente trabajo busca actualizar al lector en relación a la protección vigente que presta el ordenamiento jurídico colombiano sobre los datos personales con la reciente expedición de la ley 1581 de 2012 y su decreto reglamentario, el 1377 de 2013, de tal manera que tenga conocimiento sobre sus derechos, deberes y la manera de ejecutarlos.

2. DERECHO FUNDAMENTAL AL HABEAS DATA

2.1 QUE ES UN DERECHO FUNDAMENTAL Y SU IMPORTANCIA

Varias de las razones por las cuales es importante establecer un derecho como fundamental son, 1) Determinar cuándo es factible su protección mediante acción de tutela; 2) para establecer cuando su regulación normativa debe hacerse mediante ley Estatutaria y no ley Ordinaria, de acuerdo al artículo 152 de la Constitución; 3) Fijar los derechos que no pueden ser suspendidos durante los estados de excepción; 4) Establecer la intervención de un Juez de garantías dentro de un proceso penal, cuando se hace uso de una medida cautelar, entre otras.

Es por eso, importante tratar por lo menos de dar una definición, o establecer las características de las cuales gozan los derechos fundamentales.

Los derechos fundamentales, no son otros sino, aquellos derechos humanos que han alcanzado dos requisitos esenciales: a) el reconocimiento explícito o implícito en textos constitucionales vigentes, y b) para su defensa han sido blindados con el máximo nivel de garantías (institucionales sustantivas y judiciales) que el derecho puede hoy otorgar[3].

El primero de estos requisitos requiere que el derecho provenga de la Constitución, o de otra norma ya sea nacional o internacional que tenga rango, fuerza y valor constitucional, esto es, normas que hacen parte del bloque de constitucionalidad. Es en este orden de ideas en el que se puede evidenciar que los derechos fundamentales son derechos humanos que han sido positivados en el rango constitucional, y de esta manera, logran un alto grado de certeza y de garantía.

[3] CHINCHILLA, Tulio, ¿Qué son y cuáles son los derechos fundamentales? Segunda edición. Bogotá: Editorial Temis, p. 104.

En consonancia con lo anterior, establece el constitucionalista español Antonio Pérez Luño: “Los derechos humanos suelen venir entendidos como un conjunto de facultades e instituciones que, en cada momento histórico, concretan la dignidad, la libertad, y la igualdad humanas, las cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nivel nacional e internacional. En tanto que la noción de los derechos fundamentales se tiende a aludir a aquellos derechos humanos garantizados por el ordenamiento jurídico positivo, en la mayor parte de los casos en su normativa constitucional y que suelen gozar de una tutela reforzada”[4]

El análisis para saber la fundamentalidad de un derecho, no puede quedarse con el estudio del primer requisito, a saber, el reconocimiento en textos constitucionales. La razón de lo anterior es que la Constitución consagra una gran diversidad de derechos, de diferentes tipos y con grados de garantías disímiles. En este orden de ideas, y como lo dice el Dr. Tulio Chinchilla, la funda mentalidad de un derecho debe basarse, además de la consagración en un texto constitucional, en la protección reforzada.

Este requisito, cobra un papel de vital importancia cuando entramos a diferenciar los distintos derechos consagrados en el texto constitucional. Pues, todos éstos, al estar dentro de éste, ostentan el grado de derecho constitucional, pero no por ello, ostentan el grado de derecho fundamental. Es entonces en este momento que cobra importancia el segundo requisito, pues para recibir el tratamiento jurídico-positivo de fundamentales, los derechos constitucionales deben reunir un requisito adicional, a saber, estar dotados de una supergarantía o garantía reforzada o ser susceptible de ella[5].

[4] PÉREZ LUÑO, Antonio. Los derechos fundamentales. Madrid: Tecnos, 1998, p. 44.
[5] CHINCHILLA, Op. Cit., p. 113.

2.2 DERECHO FUNDAMENTAL PARA LA CORTE CONSTITUCIONAL

En este apartado se expondrá los lineamientos que la Corte Constitucional ha planteado para entender y determinar el alcance de un derecho fundamental de manera general, sin entrar a estudiar el derecho fundamental al habeas data, pues éste estudio será estudiado en otro apartado.

Con la claridad de lo anterior se inicia por indicar que, La Constitución de 1991 trae a su interior en el título II capítulo I “De los derechos fundamentales”, y se podría llegar a concluir que son sólo los que están en este capítulo los derechos denominados como fundamentales, pero está claro que para la Corte Constitucional, quien interpreta la Carta Magna no es así, pues reiteradamente se evidencia como se consideran otros derechos por fuera de este capítulo como fundamentales como son el derecho a la salud (art 49), derecho a la vivienda digna (art51), derecho a la seguridad social (art 48), entre otros. Así pues el presente apartado busca explicar qué entiende la Corte por derecho fundamental, evidenciar el por qué de esta categoría especial.

La Corte Constitucional a lo largo de toda su jurisprudencia ha destacado algunas características esenciales de los derechos fundamentales, más concretamente en la sentencia T- 406 de 1992, M.P CIRO ANGARITA BARÓN donde Solicita el accionante que se tutele el derecho a la salubridad pública consagrado en el artículo 88 de la Constitución Nacional. Agrega, además, que el derecho al medio ambiente sano y a la salud de la población puede estar protegido por la tutela cuando se instaura como mecanismo transitorio para evitar un perjuicio irremediable, lo anterior debido a que Las Empresas Públicas de Cartagena iniciaron en 1991 la construcción del servicio de alcantarillado para el barrio Vista Hermosa de esa ciudad. Transcurrido un año y sin haber terminado su construcción fue puesto en funcionamiento, hecho este que produjo el desbordamiento de aguas negras por los registros, ocasionando olores

nauseabundos y contaminantes de la atmósfera de los residentes tanto del barrio en mención como del Campestre, ubicado a pocos metros de aquél. A pesar de los varios requerimientos hechos a las Empresas para que terminen la obra, esta no se había concluido. Así pues habiendo hecho una breve descripción de los hechos la Corte hace un análisis de qué es un estado social de derecho, los principios fundamentales de éste y qué es un derecho fundamental. Frente a esto último la Corte indica en la sentencia T-406 de 1992, que para que un derecho tenga la calidad de fundamental debe reunir unos requisitos esenciales los cuales son:

1). Conexión directa con los principios

"La movilidad del sentido de una norma se encuentra limitada por una interpretación acorde con los principios constitucionales. Los derechos fundamentales son, como todas las normas constitucionales, emanación de los valores y principios constitucionales, pero su vinculación con estos es más directa, más inmediata, se aprecia con mayor evidencia. Todo derecho fundamental debe ser emanación directa de un principio" [6] . Estos principios se encuentran enunciados en el titulo primero de la Constitución Política de Colombia, por ejemplo tenemos: reconocimiento de la dignidad humana, el pluralismo, la democracia (en la que incluiremos los principios de participación, representación y soberanía popular), y la preservación del patrimonio cultural y natural.

Así pues se puede hacer la conexión directa por ejemplo entre el derecho fundamental a la vida, la libertad y la salud con el principio de la dignidad humana, o el derecho al voto con el principio de la democracia.

2). Eficacia directa

[6] Sentencia T-406 de 1992. M. P. Dr. CIRO ANGARITA BARÓN.

"Para que un derecho constitucional pueda ser considerado como fundamental, debe además ser el resultado de una aplicación directa del texto constitucional, sin que sea necesario una intermediación normativa; debe haber una delimitación precisa de los deberes positivos o negativos a partir del sólo texto constitucional. Por lo tanto, en normas que poseen una "textura abierta", como por ejemplo las que establecen meros valores constitucionales, a partir de la cual el legislador entra a fijar el sentido del texto, no podrían presentarse la garantía de la tutela. Está claro que no puede ser fundamental un derecho cuya eficacia depende de decisiones políticas eventuales.[7]" Esto quiere decir que el contenido de un derecho fundamental está delimitado única y exclusivamente por la carta constitucional, y por su único interprete la Corte Constitucional, ningún otro órgano puede entrar manipular su contenido. Así pues la aplicación de un derecho fundamental emana de lo que dice la carta magna y su intérprete exclusivo.

"…Es importante tener en cuenta que la eficacia de las normas constitucionales no se puede determinar en abstracto; ella varía según las circunstancias propias de los hechos: una norma de aplicación inmediata (art. 85) puede tener mayor o menor eficacia dependiendo del caso en cuestión; lo mismo un valor o un principio. El juez debe encontrar, en la relación hecho-norma la decisión más razonable, no sólo desde el punto de vista jurídico sino también desde el punto de vista fáctico.

De acuerdo con esto, la enumeración del artículo 85 no debe ser entendida como un criterio taxativo y excluyente. En este sentido es acertado el enfoque del artículo segundo del decreto 2591 de 1991 cuando une el carácter de tutelable de un derecho a su naturaleza de derecho fundamental y no a su ubicación…[8]" (Subrayado propio)

[7] Ibid, sentencia T-406 de 1992. M. P. Dr. CIRO ANGARITA BARÓN.
[8] Ibid, sentencia T-406 de 1992. M. P. Dr. CIRO ANGARITA BARÓN.

Así entonces lo que se quiere decir con eficacia directa consiste en que su aplicación emana directamente del texto constitucional, que no hay lugar a interpretaciones ni intermediaciones salvo de la Corte Constitucional y de los jueces en general cuando resuelven las tutelas, pues bajo esta labor se vuelven jueces constitucionales. También es importante tener presente que no se puede reducir esta característica de eficacia directa a los derechos enunciados en el artículo 85 de la Carta, pues nada obsta para que un derecho no enunciado en éste goce de eficacia directa a partir del análisis de los hechos y de la conexidad con otros derechos que si sean fundamentales.

3). El contenido esencial

“Existe un ámbito necesario e irreductible de conducta que el derecho protege, con independencia de las modalidades que asuma o de las formas en las que se manifieste. Es el núcleo básico del derecho fundamental, no susceptible de interpretación o de opinión sometida a la dinámica de coyunturas o ideas políticas. El concepto de "contenido esencial" es una manifestación del iusnaturalismo racionalista del siglo XVIII, según el cual, existe un catálogo de derechos anteriores al derecho positivo, que puede ser establecido racionalmente y sobre el cual existe claridad en cuanto a su delimitación conceptual, su titularidad y el tipo de deberes y obligaciones que de él se derivan.

Según esto, quedan excluidos aquellos derechos que requieren de una delimitación en el mundo de las mayorías políticas. Los derechos sociales, económicos y culturales de contenido difuso, cuya aplicación está encomendada al legislador para que fije el sentido del texto constitucional, no pueden ser considerados como fundamentales, salvo aquellas situaciones en las cuales en un

caso específico, sea evidente su conexidad con un principio o con un derecho fundamental.[9]" (Subrayado propio)

El contenido esencial es aquello que también se conoce como el núcleo esencial del derecho, es aquello que hace parte de la esencia del derecho mismo y que de llegar a vulnerarse en lo más mínimo daría como consecuencia la protección inmediata del derecho.

Así entonces estas son las características de un derecho fundamental, debe conectarse con los principios constitucionales, su protección emana directamente de la carta magna y de su intérprete oficial, y finalmente tiene un contenido esencial y vital para su existencia que no puede cambiarse por coyunturas o ideas políticas del momento. Este contenido solo puede ser ampliado por la Corte Constitucional, pues como consecuencia del crecimiento de la sociedad cada vez se hace más necesaria ampliar estos contenidos, debido a que nacen nuevas formas de vulnerar los derechos fundamentales.

2.3 EVOLUCIÓN DEL DERECHO AL HABEAS DATA

En este apartado es importante resaltar que en nuestro país el desarrollo de este derecho ha sido esencialmente jurisprudencial. Lo anterior, debido a que si bien es cierto que este derecho lo consagra la Carta Superior, ésta no lo llena de contenido y en Colombia solo hasta el 2008 se expidió la primera ley, la ley 1266 sobre habeas data, y ésta de carácter sectorial, pues su objeto indica:

> *Artículo 1°. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección,*

[9] Ibid, sentencia T-406 de 1992. M. P. Dr. CIRO ANGARITA BARÓN.

> *tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política,* ***particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.*** *(Negrilla fuera del texto original).*

Nótese que se enfatiza directamente sobre una categoría de datos particulares que son los financieros, crediticios, comerciales, de servicios y provenientes de terceros países, lo cual hace que sea una ley que regula de manera parcial el derecho al habeas data, pues qué pasa con los datos que no son de esta naturaleza. El legislador consciente del crecimiento del poder informático y que esta ley no cobijaba todos los datos, en el 2012 se expide la ley 1581 la cual si regula de manera completa el derecho al habeas data, pues su objeto indica:

> Artículo 1°. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Se evidencia así que se regula de manera completa el derecho al habeas data, ya que a diferencia de la ley 1266 de 2008, está no se enfoca en ninguna categoría de datos, por el contrario aborda todo el derecho de manera íntegra. Así entonces en la actualidad Colombia presenta un modelo hibrido en la protección de datos personales, pues de un lado esta una ley sectorial como la 1266 de 2008 y sus decretos, y de otro más general la ley 1581 de 2012 y sus decretos. La Corte Constitucional reconoce este modelo hibrido en la sentencia C- 748 de 2011:

> *…en el caso colombiano, el proyecto de ley que dio lugar a la Ley 1266 de 2008 y que fuera objeto de la sentencia C-1011 de 2008, buscaba convertirse en una ley de principios generales aplicable a todas las categorías de datos personales, pero pese a su pretensión de generalidad, el proyecto de ley en realidad solamente establecía estándares básicos de protección para el*

dato financiero y comercial destinado a calcular el nivel de riesgo crediticio de las personas. Por ello en la referida sentencia, la Corte dejó claro que la materia de lo que luego se convertiría en la Ley 1266 es solamente el dato financiero y comercial. Por lo tanto, la Ley 1266 solamente puede ser considerada una regulación sectorial del habeas data. Ahora, con el nuevo proyecto de ley se busca llenar el vacío de estándares mínimos de protección de todos los datos personales, de ahí que su título sea precisamente "Por el cual se dictan disposiciones generales para la protección de datos personales", concluyéndose que con la introducción de esta reglamentación general y mínima aplicable en mayor o menor medida a todos los datos personales, el legislador ha dado paso a un sistema híbrido de protección en el que confluye una ley de principios generales con otras regulaciones sectoriales, que deben leerse en concordancia con la ley general, pero que introduce reglas específicas que atienden a la complejidad del tratamiento de cada tipo de dato…(Subrayado fuera del texto original).

Habiendo dejado claro el modelo hibrido de protección de datos y la evolución legislativa del derecho al habeas data, resulta importante pasar a analizar la evolución en el contenido del derecho mismo, qué se entiende y qué se protege al hablar de habeas data, para lo cual se hace necesario ver la evolución que ha tenido éste a través de la jurisprudencia de la honorable Corte Constitucional.

Así entonces, este derecho está consagrado en el artículo 15 de la Constitución Política que establece "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas (…)". Este precepto constitucional, consagra tres derechos fundamentales autónomos, a saber, intimidad, buen nombre y habeas data. Este último más específicamente al indicar: *"… De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y archivos de entidades públicas y privadas…"*. Pero como bien se dijo anteriormente, esta definición no desarrolla completamente este

derecho, y por ende la Corte Constitucional lo ha tenido que llenar de contenido a través de su jurisprudencia. En una primera interpretación esta Corte entiende que la voluntad del Constituyente al introducir el derecho al Habeas Data es garantizar el derecho a la intimidad, no sólo porque ambos derechos se encuentran en el mismo artículo superior, sino porque se entiende que al hacer uso del derecho al Habeas Data se está buscando proteger la intimidad de las personas. Así lo indica la Corte cuando se refiere al derecho a la intimidad en la Sentencia T-414 de 1992:

> …particular naturaleza suya determina que la intimidad sea también un derecho general, absoluto, extrapatrimonial, inalienable e imprescriptible y que se pueda hacer valer "erga omnes", vale decir, tanto frente al Estado como a los particulares. En consecuencia, toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada. Su finalidad es la de asegurar la protección de intereses morales; su titular no puede renunciar total o definitivamente a la intimidad pues dicho acto estaría viciado de nulidad absoluta… (Negrilla fuera de texto original).

Así entonces se evidencia que a través del Habeas Data se podría garantizar el derecho a la intimidad, ya que al "*conocer, actualizar y rectificar las informaciones"* personales que reposen en una base de datos, se estaría defendiendo la intimidad. Por otro lado y también en los inicios de la Constitución se encuentra otra línea interpretativa que considera al Habeas Data una manifestación del libre desarrollo de la personalidad, ésta línea se evidencia en la Sentencia T-340 de 1993 al referirse al artículo 15 de la Constitución:

> …estableció de manera expresa la posibilidad, para todas las personas, de excluir del conocimiento público aquellos acontecimientos que, por su propia naturaleza o por la simple voluntad de ellas, deben permanecer en la esfera privada de quien los produce. Ya sea con la finalidad de impedir la averiguación indebida o la publicidad, de los sucesos que válidamente pueden mantenerse en el contorno individual de las personas....

Se nota así que a través del Habeas Data las personas desarrollan su personalidad, pues a través de éste pueden determinar qué datos personales pueden estar o no en conocimiento público.

Posteriormente, se ha construido una última interpretación que se ha sostenido hasta el día de hoy, ésta considera al habeas data un derecho autónomo. La Corte Constitucional ha señalado que el derecho al habeas data, consagrado en el artículo 15 de la Constitución Política, constituye un derecho fundamental claramente diferenciado del derecho a la intimidad y el buen nombre.[10] El núcleo esencial de este derecho a juicio de la Corte, está integrado por el derecho a la autodeterminación informática y por la libertad, en general, y en especial económica. La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales. Y se habla de la libertad económica, en especial, porque ésta podría ser vulnerada al restringirse indebidamente en virtud de la circulación de datos que no sean veraces, o que no haya sido autorizada por la persona concernida o por la ley.[11]

Así entonces este derecho hoy en día confiere tres facultades concretas a la persona a la cual se refieren los datos recogidos o almacenados: a) El derecho a conocer las informaciones que a ella se refieren; b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos; c) El derecho a rectificar las informaciones que no correspondan a la verdad.[12] Además se desprenden no solamente las facultades de conocer, actualizar y rectificar las actuaciones que se hayan recogido sobre el titular, sino también otras como autorizar el tratamiento, incluir nuevos datos, o excluirlos o suprimirlos de una base de datos o archivo.[13] Lo anterior, debido a que si bien la Carta Constitucional sólo nombra unas facultades, el mundo es cambiante, y se hacen necesarias

[10] CORTE CONSTITUCIONAL. Sentencia T-176 de 1995, M.P. Eduardo Cifuentes Muñoz, p. 4
[11] Ibid, sentencia SU-082 de 1995
[12] Ibid, sentencia SU-082 de 1995
[13] Ibid, sentencia C-748 de 2011, p. 85

nuevas facultades de las que gocen los titulares en relación con sus datos, de tal manera que las facultades descritas en la Constitución o en la Ley no se pueden entender como taxativas. Un derecho nunca se podrá definir y delimitar completamente, así tampoco las facultades que involucra, puesto que acorde se manifiesten nuevas amenazas y violaciones en la sociedad habrá que ampliar ese marco de facultades para garantizar su protección

2.4. VULNERACIÓN DEL DERERCHO AL HABEAS DATA

Como derecho fundamental que es, el habeas data puede ser vulnerado por diferentes personas –naturales o jurídicas- y de diversas maneras. Es por esta razón que se han creado diferentes mecanismos de protección de éste derecho.

La jurisprudencia constitucional, se ha encargado de exponer los casos en los cuales resulta vulnerado el derecho al habeas data, y ha encontrado básicamente tres casos en los cuales se vulnera este derecho.

Esta postura la ha reiterado la Corte Constitucional en diferentes sentencias, a lo largo de la vigencia de la Constitución Política de 1991, es así como en la sentencia T-176 de 1995 expone: "*Para que exista una vulneración del derecho al habeas data, la información contenida en el archivo debe haber sido recogida de manera ilegal, sin el consentimiento del titular del dato (i), ser errónea (ii) o recaer sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente (iii).*"

En el mismo sentido de la anterior, la sentencia T-067 del 2007, y la sentencia T-658 de 2011 dicen que: *"El derecho al habeas data resulta vulnerado en los eventos en que la información contenida en un archivo de datos (i) sea recogida de forma ilegal, (ii) sea errónea, (iii) o verse sobre aspectos reservados de la esfera personal del individuo".*

Es importante señalar en este punto, que la misma corporación ha entendido que en los casos en que la información contenida sea errónea, se está afectando el derecho al buen nombre, puesto que se está presentando una información equivocada, que no corresponde con la imagen que la persona ha trabajado para tener frente a la sociedad.

En conclusión, siguiendo los lineamientos de la Honorable Corte Constitucional, el derecho de habeas data potencialmente se vulnera de tres maneras, y estas son:

- Cuando la información sea recogida de manera ilegal.

  La Corte Constitucional ha relacionado el principio de libertad, con la prohibición del manejo de la información adquirida de manera ilícita, de tal forma que se encuentra prohibida la obtención y divulgación de los mismos, sin la previa autorización del titular o en ausencia de mandato legal o judicial. Así, en la sentencia SU-082 de 1995, afirmo “los datos conseguidos, por ejemplo, por medios ilícitos no pueden hacer parte de los bancos de datos y tampoco pueden circular.” En el mismo sentido, en la sentencia T-176 de 1995, se consideró como una de las hipótesis de la vulneración del derecho al habeas data el de la recolección de la información “de manera ilegal, sin el consentimiento del titular de dato.” Así entonces, se puede concluir acorde a lo anterior que recoger y tratar información de manera ilegal es no contar con la autorización previa, expresa e informada del titular del dato.

- Cuando la información sea errónea.

  Este punto tiene conexión directa con el principio de veracidad, el cual indica que la información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible, además se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error. Resulta

importante destacar el actuar del titular, pues es éste quien tiene la carga de otorgar datos con las características anteriormente enunciadas. Lo anterior adquiere relevancia en el caso en el que el titular entregue datos al responsable que no sean veraces, y éste los trate con el convencimiento de que son los correctos. En este caso, el responsable no vulnera el derecho del titula, pues éste contaba con la autorización previa, expresa e informada del titular y la responsabilidad, en principio, recaería exclusivamente sobre el titular.

- Cuando la información trate de aspectos privados de la esfera personal.

  Esto tiene relación con la categoría de dato sensible, desarrollado en el artículo 5° de la Ley 1581 de 2012, artículo que establece que un dato sensible es aquel que afecte la intimidad del titular, o aquel cuyo uso indebido pueda generar discriminación. El tratamiento de estos datos está prohibido por regla general, prohibición que se ajusta a la Carta Política, así lo confirma la Corte Constitucional en la sentencia C-748 de 2011:

  > …de la misma manera, la prohibición de su tratamiento, como regla general, no solamente es compatible con la Carta, sino que es una exigencia del derecho a la intimidad y un desarrollo del principio del habeas data de acceso y circulación restringida....

Esta regla general tiene cuatro excepciones creadas por la misma Ley 1581, en su artículo 6°, a saber i) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización; ii) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización; iii) El Tratamiento sea efectuado en el curso de actividades legítimas y con las debidas garantías por parte de la fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa, o sindical,

siempre que se refieran exclusivamente a sus miembros o las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos se podrán suministrar a terceros sin la autorización del Titular; iv) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Esto tiene su justificación, en el sentido que los datos sensibles versan sobre los aspectos más personales e íntimos de los Titulares, información que si se llega a divulgar a terceros (exceptuando los numerales del artículo 6° de la Ley antes mencionada) podrían acarrear graves consecuencias para el Titular, consecuencias como discriminación, burlas, o en algunos casos, llegar a ser víctimas de agresiones, físicas o verbales.

2.5 LA TUTELA COMO MECANISMO DE PROTECCIÓN DELDERECHO AL HABEAS DATA

En el ordenamiento Jurídico Colombiano existen varios medios para salvaguardar y proteger nuestros derechos en distintas ramas del derecho como es la penal, civil, laboral, entre otras. Es importante resaltar la posibilidad de que un mismo conflicto pueda verse envuelto en una o más jurisdicciones. Concretándonos en los conflictos relacionados con datos personales nótese que se puede presentar la protección mediante distintos mecanismos como sería en el área laboral cuando el empleador hace mal uso de los datos, si está deteriorando el buen nombre se puede acudir a instancias penales por calumnia, también se puede iniciar un trámite de consulta o reclamo ante el responsable y/o encargado del tratamiento, se puede elevar queja ante la superintendencia de industria y comercio, y en último caso cuando se busca proteger de manera rápida derechos fundamentales se puede acudir al mecanismo constitucional de la tutela.

En la actualidad, el medio más invocado es la tutela, razón por la cual si bien se enuncian varios mecanismos de defensa para proteger los derechos que se ven involucrados en la protección de datos personales, se hará un análisis de la tutela como mecanismo para la protección de datos personales y determinar la viabilidad y en qué casos se podría invocar dicho instrumento.

El objeto de la acción de tutela es la protección de los derechos fundamentales. Esta acción, puede ser interpuesta por cualquier persona que esté siendo vulnerada en sus derechos fundamentales y procederá contra autoridades públicas y contra particulares cuando se presente una de las siguientes tres circunstancias: i) estén prestando un servicio público, ii) su conducta afecte gravemente un interés colectivo, iii) cuando el solicitante se halle en un estado de subordinación o indefensión. El primero de los tres supuestos es de naturaleza objetiva, mientras que los dos restantes son de naturaleza subjetiva y por tanto la procedencia de éstos, deberá ser analizada en cada caso concreto.

Para hablar de la tutela como un medio para la protección de derechos fundamentales se debe hablar del decreto 2591 de 1991 el cual en su artículo 6 señala las causales de improcedencia de la tutela, de las cuales para la protección de datos personales interesa la siguiente:

> ARTICULO 6º. CAUSALES DE IMPROCEDENCIA DE LA TUTELA. La acción de tutela no procederá:
>
> e) Cuando existan otros recursos o medios de defensa judiciales, salvo que aquélla se utilice como mecanismo transitorio para evitar un perjuicio irremediable. La existencia de dichos medios será apreciada en concreto, en cuanto a su eficacia, atendiendo las circunstancias en que se encuentra el solicitante…

El derecho del habeas data, como derecho fundamental[14] goza de ésta protección de la acción de tutela.

[14] Así lo entiende la Corte Constitucional, y en la sentencia C-748 de 2011, expresa: "…*Este derecho como fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben pender de los jueces, sino de*

Por otro lado, ya enfocándose en la protección de datos personales cuando los particulares hacen un uso indebido de ellos, el artículo 42 # 7 de este decreto dispone:

> ARTICULO 42. PROCEDENCIA. La acción de tutela procederá contra acciones u omisiones de particulares en los siguientes casos:
>
> 7. Cuando se solicite rectificación de informaciones inexactas o erróneas. En este caso se deberá anexar la transcripción de la información o la copia de la publicación y de la rectificación solicitada que no fue publicada en condiciones que aseguren la eficacia de la misma…

Es evidente que en todos los casos existen recursos o medios de defensa diferentes a la tutela, pero ¿cómo saber cuándo se puede usar la tutela como mecanismo transitorio para evitar un perjuicio irremediable? ¿Cuándo los datos pueden causar un perjuicio de tal magnitud? ¿Se debe esperar al contenido consagrado por el #7 del Artículo 42 anteriormente citado para poder hacer uso de la tutela?

Resulta difícil e inclusive casi imposible dar una respuesta general y objetiva a las preguntas anteriormente hechas, debido a que como dice el artículo 6 del decreto 2591 de 1991 "*La existencia de dichos medios será apreciada en concreto, en cuanto a su eficacia, atendiendo las circunstancias en que se encuentra el solicitante…"*. De tal manera que habría que entrar analizar cada caso concreto para determinar si se puede hacer uso de la tutela o no. Hay que determinar también las condiciones del accionante y el objetivo que busca éste con la tutela.

Se debe analizar el objetivo que busca el accionante para determinar la procedencia de la tutela, puesto que en muchos casos su interés no es buscar una indemnización, que se perjudique y sancione a la empresa, o que al responsable

---

una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones."

se le castigue penalmente, sino que en muchos casos lo que busca la persona es la simple protección de sus derechos fundamentales y no la sanción para los responsables o una indemnización. Esto se evidencia en la Sentencia T- 787-04 donde la Corte Constitucional analiza la procedencia de una tutela, de una persona a la que le hicieron una caricatura burlesca y mostrando aspectos personales de ella, publicando ésta en una revista. La persona buscaba a través de la tutela que se ordenara quitar la caricatura e indicar que la misma no era real, en esta Sentencia la Corte indica:

> …Sin embargo, la simple existencia de una conducta típica que permita salvaguardar los derechos fundamentales, no es un argumento suficiente para deslegitimar per se la procedencia de la acción de tutela, pues bien puede suceder que la afectación exista y siendo antijurídica simultáneamente concurra cualquier presupuesto objetivo o subjetivo que excluya la responsabilidad criminal, lo cual conduciría a la imposibilidad de brindar cabal protección a los derechos del perjudicado. De igual manera, puede suceder que la víctima no pretenda el castigo penal del agresor, sino tan sólo persiga su inmediata rectificación, finalidad para la cual el trámite de una acción penal resultaría in extremo dispendiosa. Por otra parte, la inmediatez de la acción de tutela, impediría que los efectos de una difamación sigan expandiéndose y prologándose en el tiempo como acontecimientos reales y fidedignos, lo cual difícilmente puede lograrse con la acción penal que simplemente culminaría con la imposición de una pena luego de un extenso proceso. Por ello, esta Corporación ha reconocido que en tratándose de la vulneración de derechos fundamentales, tales como, el buen nombre, la intimidad y la honra, el uso de la acción criminal, no excluye el ejercicio autónomo la acción de tutela, pues no son los mismos los objetivos que se persiguen, ni idéntica la finalidad de la sanción y, menos aún, concurrentes sus supuestos o constantes de responsabilidad…

La Corte Constitucional, se ha pronunciado al respecto y ha establecido que:

> En el caso de la procedencia de la acción de tutela para invocar el amparo del derecho fundamental al habeas data, esta Corporación ha fijado como requisito previo que el peticionario haya acudido a la entidad correspondiente para corregir, aclarar, rectificar o actualizar la información que se tenga de él, conforme se desprende del contenido del artículo 42, numeral 6° del Decreto 2591 de 1991.
>
> En este mismo sentido, el numeral 6° del literal II del artículo 16 de la Ley Estatutaria 1266 de 2008, preceptúa: ‘Sin perjuicio del ejercicio de la acción de tutela para amparar el derecho fundamental del hábeas data, en caso que el

> titular no se encuentre satisfecho con la respuesta a la petición, podrá recurrir al proceso judicial correspondiente dentro de los términos legales pertinentes para debatir lo relacionado con la obligación reportada como incumplida (…)'
>
> Es decir que la acción de tutela es el mecanismo procedente para solicitar el amparo del derecho fundamental al habeas data contra un particular, cuando se evidencia el estado de indefensión frente al mismo y se verifica que el peticionario elevó la correspondiente solicitud de aclaración, corrección, rectificación o actualización del dato ante la entidad correspondiente[15].

Acorde a lo anterior, no se puede determinar de manera a priori cuando se puede hacer uso de la tutela como mecanismo para proteger los derechos fundamentales que se derivan de la protección de datos que serían por ejemplo el derecho a la intimidad, al bueno nombre, al habeas data, entre otros. Hay que analizar caso por caso qué se pretende proteger, qué mecanismos existen y en qué condiciones está el accionante, y de esta manera determinar si hay lugar a la protección vía acción de tutela.

[15] Ibid, sentencia T-658 de 2011. M. P. Dr. Jorge Ignacio Pretelt Chaljub.

3. DATO PERSONAL Y SU PROPIEDAD

La Ley 1581 del 2012, define el dato personal, como “cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”. Asimismo, el decreto reglamentario 1377 de 2013, introduce dos categorías de datos, a saber: dato público y dato sensible. Entendiendo por el primero dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva; y por el segundo aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Teniendo clara la definición anterior se puede concluir que existen diferentes clases de datos, por ejemplo, de identificación (nombre, domicilio, teléfono, correo electrónico, firma, fecha de nacimiento, edad, nacionalidad, estado civil, etc.); laborales (puesto, domicilio, correo electrónico y teléfono del trabajo); patrimoniales (información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos, etc.); académicos (trayectoria educativa, título, número de cédula, certificados, etc.); ideológicos (creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas; de salud (estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, etc.); características

personales (tipo de sangre, ADN, huella digital, etc.); características físicas (color de piel, iris y cabellos, señales particulares, etc.); vida y hábitos sexuales, origen (étnico y racial.); entre otros.[16] Pero qué es un dato personal, por qué es tan relevante, una respuesta a esto se da en la Sentencia T 414 de 1992 que cita al Profesor Ernesto Lleras y dice:

> …El dato que constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto sería susceptible de usarse para coartarla, es de su propiedad, en el sentido de que tendría ciertos derechos sobre su uso. Datos de este tipo serían sus señales particulares, relaciones de propiedad y de familia, aspectos de su personalidad, y señales de identidad de diversa índole que van emergiendo en las actividades de la vida. Todos estos datos combinados en un modelo, son equivalentes a una "huella digital" porque el individuo es identificable a través de ellos.
>
> Por las características propias de los datos, una vez producidos (codificado un evento u objeto por alguien o eventualmente una máquina) pueden diseminarse con relativa facilidad. Esto hace que puedan ser usados, en combinación con otros de procedencias distintas pero adscribibles a la misma persona. Así se va configurando lo que ha dado en llamar un "perfil de datos de una persona"(Lleras). Estos perfiles pueden construirlos quienes tengan bancos de datos bien sea manuales o sistematizados, y el poder de información y control social que estos tengan depende del uso de la tecnología disponible.
>
> El problema del "poder informático" existe siempre que se poseen datos sobre las personas bien sea en forma manual o por medios electrónicos. Con el desarrollo de estos últimos, las posibilidades de acción de ese poder en contra de la libertad de las personas se magnifican y harían necesaria una legislación especial.
>
> El "perfil de datos" de la persona se constituye entonces en una especie de "persona virtual" sobre la cual pueden ejercerse muchas acciones que tendrán repercusión sobre la persona real. Desde el envío de propaganda no solicitada, hasta coerción u "ostracismo" social como en el caso que se presenta. Un "buen" manejo de Bancos de Datos permitiría identificar hasta perfiles poblacionales desde distintos puntos de vista, lo cual constituye un evidente peligro de control social de aquellos que ostentan "poder informático", no solamente contra la libertad de las personas individuales sino contra la de sectores sociales más amplios… (Subrayado propio).

[16] http://blog.derecho-informatico.org/faqs/datos-personales/

En la manipulación de datos pueden intervenir varias personas. Uno es el sujeto del cual se dice algo o al cual algo le concierne en el universo informativo construido a partir del dato. Otro es el sujeto que, aplicando unos códigos o gramáticas como instrumentos auxiliares, hace que el dato se convierta en información. Pueden existir otros cuya labor específica es la circulación y difusión de la información con destino a los clientes habituales de los medios de comunicación. La labor primordial de estos últimos sujetos es, como se ve, hacer que el dato se convierta en esa mercancía denominada a veces noticia, apta para el consumo de su clientela que las nuevas tecnologías de información permiten ampliar más y más cada día. En estas condiciones, los diversos sujetos son apenas titulares de algunas facultades que no les confieren necesariamente la calidad de propietarios. Muchas veces no son más que simples depositarios forzosos.[17]

De lo anterior es importante resaltar, que una vez transformada ese dato en información se puede comercializar, es un negocio, una mercancía, es un poder. Esto se demuestra en la compra y venta que se hace de bases de datos, y la cláusula de confidencialidad que se pacta en los contratos civiles y comerciales, con el fin de proteger la información. Por otro lado, la Corte Constitucional ha establecido unos criterios para determinar qué datos personales son íntimamente privados y por ende relacionarse directamente con el derecho a la intimidad y gozar de una especial protección y de otro lado los datos personales que tienen relevancia pública y por ende relacionados con el derecho a la información de las demás personas, esto está en la Sentencia T-261 de 1995:

> … De los datos personales-concepto genérico- hacen parte todas aquellas informaciones que atañen a la persona y, por tanto, pueden ser, junto con las estrictamente reservadas, las referentes a aspectos que relacionan a la persona con la sociedad y que, por tanto, son públicas. Así, por ejemplo, no puede equipararse la información referente a una disputa típica e indudablemente conyugal, que sólo importa a los esposos, con el dato, también personal pero relevante social y aun jurídicamente, que alude al

[17] Ibid, sentencia T 414 de 1992, M.P. Ciro Angarita Barón

> hecho de haber desempeñado cierto cargo o de poseer un determinado vehículo.
>
> De tal modo, hay datos personales que específicamente son íntimos y gozan, en consecuencia, de la garantía constitucional en cuanto tocan con un derecho fundamental e inalienable de la persona y de su familia, al paso que otros, no obstante ser personales, carecen del calificativo específico de privados, toda vez que no únicamente interesan al individuo y al círculo cerrado de su parentela, sino que, en mayor o menor medida, según la materia de que se trate, tienen importancia para grupos humanos más amplios (colegio, universidad, empresa), e inclusive para la generalidad de los asociados, evento en el cual son públicos, y si ellos es así, están cobijados por otro derecho, también de rango constitucional fundamental, como es el derecho a la información…

Lo anterior, no significa que se puede eximir o pasar por alto pedir la autorización del titular del dato cuando se vaya a tratar datos personales de carácter público, pues nótese que sigue siendo un dato personal. De tal manera que su naturaleza no se pierde y se sigue necesitando la autorización, además de cumplir con los demás requisitos legales, lo único es que dichos datos no gozan de igual protección que los datos personales de naturaleza privada e íntima.

Es importante resaltar que, como lo indica el profesor Ernesto Lleras, al tratar los datos personales de una persona si bien no se está tratando directamente a la persona física, se está tratando con la “persona virtual”, y lo que se haga con esta persona virtual puede llegar afectar a la persona física. Se evidencia así, que el tratamiento de datos es un actuar extremadamente delicado y que se debe hacer con las garantías y obligaciones legales y constitucionales, para evitar afectar a la persona tanto virtual como física.

Lo cierto es que por las muy estrechas relaciones entre el dato personal y la intimidad, la sola búsqueda y hallazgo de un dato no autoriza a pensar que se ha producido simultáneamente su apropiación exclusiva y, por tanto, la exclusión de toda pretensión por parte del sujeto concernido en el dato. De ahí que no pueda hablarse de que existe un propietario del dato con las mismas implicaciones como si se tratara de una casa, un automóvil o un bien intangible. Tampoco cabe pensar

que la entidad que recibe un dato de su cliente en ejercicio de una actividad económica, se convierte por ello mismo en su propietario exclusivo hasta el punto de que es ella quien pueda decidir omnímodamente su inclusión y posterior exclusión de un banco de datos. Esto sería tanto como autorizarlo de lleno a desposeer al sujeto, con todas sus consecuencias previsibles, de los "perfiles virtuales" que, como ya hemos visto, pueden construirse a partir de los datos de una persona.[18]

Con las posibilidades que ofrecen hoy las modernas tecnologías de información y, en particular, los bancos de datos computarizados, ello equivaldría también a autorizar a la persona o entidad que recibe el dato a encarcelar "virtualmente" en el banco de datos al sujeto concernido en los mismos. Lo cual, en países que carecen de una legislación específica protectora de la intimidad frente al fenómeno informático, favorecería abiertamente su cotidiana vulneración.[19] Que estos abusos no son simplemente potenciales e imaginarios, ya que en muchos casos se concreta dicha vulneración.

En definitiva, muchas entidades públicas o privadas, pueden gastar tiempo, dinero, y trabajo de sus empleados recolectando la información de las personas, pero esto no las vuelve dueñas del dato que recogieron, pues el mismo se sigue refiriendo a la persona que es titular, y por ende sólo la podrán utilizar acorde a la finalidad dada al titular y con la autorización libre, expresa y por escrito que haya dado el mismo. De tal manera que podrán comercializar los datos como un "producto no físico" pero nunca nada serán propietarios de los mismos, solamente lo será el titular sobre el cual los datos recaen o se refieren.

[18] Ibid, sentencia T 414 de 1992, M.P. Ciro Angarita Barón
[19] Ibid, sentencia T 414 de 1992, M.P. Ciro Angarita Barón

4. PRINCIPIOS DE LA PROTECCION DE DATOS

En este apartado se pasa a hablar del objeto central de este trabajo, que es la ley 1581 de 2012 y su decreto 1377 de 2013, iniciando por los principios, puesto que éstos son la base y la guía para comprender e interpretar mejor el contenido de la ley y el decreto. Los principios son un mandato de optimización que ordena que se realice algo en la mayor medida de lo posible de acuerdo con las posibilidades jurídicas y fácticas buscando impedir así el uso abusivo y arbitrario de la facultad informática. El artículo 4 de la Ley define el contexto axiológico dentro del cual debe moverse, el proceso informático. Según este marco general, existen unos parámetros generales que deben ser respetados para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo.[20]

Habiendo hecho una introducción de los principios, y habiendo resaltado su importancia se vuelve indispensable indicar el porqué de éstos, para lo cual se hace necesario traer la legislación internacional sobre el tema que fue base e inspiración del legislador para introducir y desarrollar los principios que trae la ley. Dentro de la legislación internacional pertinente y relacionada con el tema tenemos:

El sistema de protección Europeo fue el primero, en el año de 1981, en instar a los miembros de la Comunidad a adoptar en sus legislaciones internas unos principios mínimos de protección, ante el surgimiento de grandes bases de información que podían poner en riego los derechos de los ciudadanos. El artículo 5 del Convenio No. 108 del 28 de agosto establece que los datos deben regirse al amparo de las siguientes directrices:

[20] Ibid, sentencia C-748 de 2011

a) “ser obtenidos legalmente y tratados de la misma forma,

b) ser registrados para finalidades específicas y lícitas, por lo que no podrán ser utilizados con distintos fines,

c) ser adecuados, pertinentes y acordes con las finalidades para las cuales fueron previstas,

d) ser exactos y puestos al día,

e) ser conservados de tal forma que permita la identificación de las personas que fueron concernidas durante un periodo de tiempo que no exceda del necesario para el cual fue registrado.”

En los años noventa fueron adoptados dos instrumentos internacionales relacionados con el manejo de los datos. El primero, la Resolución 45/95 del 14 de diciembre de 1990 de la Organización de las Naciones Unidas, y el segundo, la Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión.

La Resolución 45/95 de la ONU, “principios rectores sobre la reglamentación de ficheros computarizados de datos personales”, dentro de los cuales desarrolla: Principio de la licitud y lealtad, Principio de exactitud, Principio de finalidad, Principio de acceso a la persona interesada, entre otros.

Por su parte, la Directiva 95/46/CE, sistematiza las directrices del manejo de los datos y reconoce que tales disposiciones se encuentran encaminadas a “la protección de las libertades y de los derechos fundamentales a las personas físicas y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de datos personales” (artículo 1). El instrumento divide los principios en dos categorías: (i) los relativos a la calidad del dato y (ii) los concernientes a la legitimidad en el manejo de la información.

En relación con los primeros dispone (artículo 6) que los datos personales sean: “(i) Tratados de manera leal y lícita, (ii) Recogidos con fines determinados,

explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas, (iii) Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente, (iv) Exactos y, cuando sea necesario, actualizados; deberán tomarse las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados, (v) Conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un periodo más largo al mencionado, con fines históricos, estadísticos o científicos."

En cuanto a los segundos, la Directiva establece que el manejo de los datos sólo puede realizarse con el consentimiento inequívoco del titular y cuando es necesario : (i) "para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales.", (ii)"para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento", (iii) "para proteger el interés vital del interesado",(iv) para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos" y (v) para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 de la presente directiva".[21]

Así pues, se evidencia como se ve influenciado el legislador por legislación internacional relacionada con el tema, pues nótese que algunos de los principios

[21] Ibid, sentencia C-748 de 2011

recogidos por estos organismos internacional guardan una estrecha relación con los que tiene la ley 1581 de 2012.

Por otro lado, en el caso Colombiano es importante indicar que los principios ya habían sido recogidos por la jurisprudencia constitucional como garantías derivadas del derecho fundamental al habeas data y, por tanto, incluso en ausencia de una ley que lo disponga, son de aplicación obligatoria al tratamiento de todo tipo de dato personal.[22] También es importante resaltar que los principios acorde al parágrafo del artículo 4 de la Ley 1581 de 2012 aplican para todas las bases de datos incluso las exceptuadas. Así también en el flujo de datos personales se enfrentan dos intereses, por un lado, la especial necesidad de disponibilidad de información mediante la conformación de bases de datos personales, por otro, el requerimiento de proteger los derechos fundamentales de los posibles riesgos del proceso de tratamiento de datos. En consecuencia, se torna indispensable someter este proceso a ciertos principios jurídicos, con el fin de garantizar la armonía entre las relaciones jurídicas[23], razón por la cual se hará un análisis de fondo de cada uno de ellos a continuación: Primero se citará el principio como lo trae la Ley y posteriormente se le dará un breve análisis.

4.1 PRINCIPIO DE LEGALIDAD EN MATERIA DE TRATAMIENTO DE DATOS

Este principio se encuentra en la ley 1581 de 2012, y se refiere a que la actividad debe ser reglada, que debe sujetarse a lo establecido en la normatividad que regule la materia.

Este principio básicamente indica que el tratamiento de datos personales se debe tratar con los límites establecidos por la Ley, de tal manera que se eviten y se prohíba el tratamiento de datos recogidos de manera ilícita y por ende por fuera

[22] Ibid, sentencia C-748 de 2011, p. 93
[23] Ibid, sentencia C.748 de 2011, p. 117

del marco de la Ley. Éste es un principio que está íntimamente ligado con el principio de licitud, pues como lo dice la Honorable Corte Constitucional en la sentencia C-748 de 2011, “El principio encierra el principal objetivo de la regulación estatutaria: someter el tratamiento de datos a lo establecido en las normas, fijar límites frente a los responsables y encargados del tratamiento y garantizar los derechos de los titulares de los mismos. En estos términos, tal y como se explicó anteriormente, a partir del principio de libertad, la jurisprudencia constitucional señaló que el dato debía ser adquirido, tratado y manejado de manera lícita.”.

4.2 PRINCIPIO DE FINALIDAD

Los datos que se tratan y/o administran deben obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada a la persona sobre la cual los datos se refieren. Acorde a lo anterior, se debe indicar el fin u objetivo que se busca con los datos a su propietario al momento en que éste otorga su consentimiento, de tal forma se debe plasmar y dejar clara la finalidad en el momento que se entrega la autorización por parte del titular.

Este principio resulta de vital importancia en materia de datos personales, ya que la autorización acorde al principio de libertad que más adelante se trata, debe ser utilizada y focalizada expresamente a la finalidad con la que se recogen los datos. De tal manera, que es importante tener presente la finalidad, pues ésta le pone un margen, un límite al tratamiento y/o administración de los datos, debido a que los datos que se tengan por fuera del ámbito de la finalidad se estarían administrando y/o tratando de manera ilícita. Así también, los datos deben ser, estar o existir en un banco de datos mientras exista la finalidad de tal forma que cuando se extinga la finalidad los datos personales deben ser excluidos. Por otro lado acorde al principio de necesidad solamente se deben tener los datos que estrictamente sean necesarios para alcanzar la finalidad descrita. En conclusión debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al

mínimo necesario. Es decir, los datos deberán ser: (i) adecuados, (ii) pertinentes y (iii) acordes con las finalidades para las cuales fueron previstos.[24]

4.3 PRINCIPIO DE LIBERTAD

Este principio se caracteriza por exigir que los datos personales de las personas, ya sean de índole económico u otro se deben administrar y/o tratar sólo y exclusivamente con el consentimiento, previo, expreso e informado del Titular, es decir, de la persona sobre la cual los datos se refieren y que por ende son de su propiedad.

Este principio, es el pilar fundamental de la administración y/o tratamiento de datos, permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos. También impide que la información ya registrada de un usuario, la cual ha sido obtenida con su consentimiento, pueda pasar a otro organismo que la utilice con fines distintos para los que fue autorizado inicialmente. [25] Así pues este principio guarda estrecha relación con la autorización que da el titular para tratar con sus datos personales acorde a la finalidad indicada, como ya se manifestó anteriormente dicha autorización debe ser previa, expresa e informada. Por otro lado, este principio se relaciona de manera directa con el derecho a la intimidad, al libre desarrollo de la personalidad y a la autodeterminación informática (habeas data). Resulta obvio pues las persona a través de su libertad y por ende de su autorización pueden determinar qué datos personales quiere que sean conocidos y cuáles no, y así proteger la intimidad, de tal manera que pueda ir construyendo su “imagen informática”, que como ya se dijo anteriormente esta “persona virtual” puede en muchos aspectos llegar afectar a la real. En conclusión, este principio de libertad y su manifestación más grande que es la autorización le dan a la persona un mecanismo de defensa ante el emergente poder informático que a cada día da pasos más grandes y poderosos,

[24] Ibid, sentencia C.748 de 2011, p. 127
[25] Ibid, sentencia C.748 de 2011, p. 127

que en muchos casos pisando y pasando por alto los derechos de las personas cuyos datos se tratan o administran.

4.4 PRINCIPIO DE VERACIDAD O CALIDAD

Sobre este principio, simplemente es importante resaltar que se impone a los bancos de datos el deber de verificar la veracidad de los mismos, lo cual es una carga bastante grande. Pero los titulares de la información también tienen el deber de entregar datos veraces.

Acorde a lo anterior, los datos personales contenidos en las bases de datos deben obedecer a situaciones reales, ser ciertos y precisos; la información que se suministre debe corresponder a la verdad, ser verídica e imparcial, y además debe ser completa, en atención al principio de integridad estrechamente vinculado al de veracidad, en virtud del cual, la información que se registre o se divulgue no puede contener datos parciales, incompletos o fraccionados. Así las cosas, si las informaciones contenidas en los bancos de datos resultan fidedignas, verídicas y completas, no puede alegarse vulneración del derecho al habeas data o al buen nombre.[26]

Este principio es altamente importante, pues al ser incumplido no solamente se ve afectado el derecho al buen nombre de las personas, sino que también se afectaría la actividad económica. En este sentido, la Corte Constitucional, en la sentencia T-094 de 1995, ha dicho: “Es claro que si la información respectiva es falsa o errónea, no solamente se afectan los derechos a la honra y al buen nombre de la persona concernida, sino que, precisamente por el efecto multiplicador que tiene el informe negativo en las instituciones receptoras de la información incorporada al banco de datos o archivo, resulta notoriamente perjudicada en su actividad económica y en su situación patrimonial. No se pierda de vista que un

[26] Ibid, sentencia T-846 de 2004, M.P. Alfredo Beltrán Sierra

cierre del crédito puede provocar una cadena de incumplimientos forzados, la incapacidad de contraer nuevas obligaciones, la cesación de pagos y la quiebra."

En concordancia con lo anterior ha dicho la Misma corporación que la transmisión de información errónea en este campo no solo afecta la buena imagen o fama que un individuo ha construido en sociedad sino que también genera un impacto negativo en la esfera económica.[27]

4.5 PRINCIPIO DE TRANSPARENCIA

Este principio consiste en que se debe garantizar el derecho del titular de la información, de obtener en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Este principio advierte que las personas que traten con datos personales deben garantizarle a los titulares el derecho a la información de sus datos cuando ellos los estimen conveniente, pero además de esto cuando se procese datos personales datos debe ofrecer, como mínimo, la siguiente información a la persona afectada: (i) información sobre la identidad del controlador de datos, (ii) el propósito del procesamiento de los datos personales, (iii) a quien se podrán revelar los datos, (iv) cómo la persona afectada puede ejercer cualquier derecho que le otorgue la legislación sobre protección de datos, y (v) toda otra información necesaria para el justo procesamiento de los datos.[28]

4.6 PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA

El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o personas previstas en la presente Ley.

[27] Ibid, sentencia T-658 de 2011, M. P. Dr. Jorge Ignacio Pretelt Chaljub.
[28] Ibid, sentencia C.748 de 2011, p. 131

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a Titulares o terceros autorizados conforme a la presente Ley.

Sobre este principio hay que decir, simplemente que para tratar datos personales se deben garantizar todas las medidas de seguridad necesarias de tal manera que sólo puedan acceder las personas autorizadas y los titulares y que se trate la misma información acorde a la finalidad previamente indicada al titular.

La norma, a saber la Ley 1581 de 2012, es muy clara al establecer cómo debe entenderse la aplicación de este principio. De esta se desprende que los datos que no son catalogados como públicos no podrán ser publicados en internet, y sólo será posible publicarlos en el caso que se otorguen todas las garantías. Todo manejo de información no pública, deberá hacerse con mucho rigor, y con la mayor seguridad posible, para evitar que terceros no autorizados puedan tener acceso a ésta.

4.7 PRINCIPIO DE SEGURIDAD

La información sujeta a tratamiento por el Responsable del tratamiento o el Encargado del tratamiento a que se refiere la presente ley, se deberá manera con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Este principio impone una obligación al Responsable y al Encargado del tratamiento a implementar medios eficaces de seguridad en la administración de datos, debido a que hay ciertos datos que debe permanecer en lo privado o que deben tener una protección mayor. De tal manera que se deben proteger los datos en mayor o menor manera dependiendo de la naturaleza de los mismos.

4.8 PRINCIPIO DE CONFIDENCIALIDAD

Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligados a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ellos corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

Este principio básicamente impone una obligación de no hacer a los que intervienen en el tratamiento de datos personales, dicha obligación consiste en no divulgar datos sin la respectiva autorización y dentro de los límites de la ley, inclusivo después de terminada la relación o una vez se consiga la finalidad.

4.9 PRINCIPIO DE INTERPRETACIÓN INTEGRAL DE DERECHOS CONSTITUCIONALES

"La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables.[29]"

4.10 PRINCIPIO DE RESPONSABILIDAD

[29] COLOMBIA. CONGRESO DE LA REPÚBLICA. 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, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

Este principio es de carácter doctrinal, es decir, no se encuentra enunciado ni desarrollado por ninguna de las leyes de habeas data. Se caracteriza por aludir a dos deberes.

1. "El deber de diligencia en el manejo de los datos: El deber de diligencia en el manejo de los datos. Un aspecto que corresponde dilucidar a la jurisdicción civil en caso de demanda por daños causados es si se trata de un responsabilidad basada en culpa probada o culpa presunta (se exonera probando que se actuó con diligencia y cuidado), o de presunción de responsabilidad (sólo se exonera probando una causa extraña: culpa de la víctima, fuerza mayor, hecho de un tercero). La Sentencia T-577/93 dice que el manejo de datos "exige de las entidades privadas y públicas que manejan estas centrales un comportamiento caracterizado por el **máximo grado de diligencia y razonabilidad"** (las negrillas son del texto), lo que es una pauta para el juez ordinario."[30]

   Así pues nótese que este principio se enfoca más en los datos regulados por la ley 1266 de 2008, pues se habla de centrales, lo que da a entender que se centra en unos datos específicos y no de carácter general. Lo que se busca esencialmente es que quienes manejen este tipo de datos tengan un máximo grado de diligencia y razonabilidad, ya que se estaría administrando datos delicados como son aquellos de carácter financiera, crediticio y de servicios. El siguiente deber también tiene relación directa con los datos regulados por la ley 1266 de 2008, como quedará en evidencia a continuación.

2. *El deber de indemnizar* consecuencialmente el daño causado: sobre este tema es preciso hacer las siguientes distinciones.

   - *"La regla general es la improcedencia de la condena al pago de perjuicios y costas en sede de tutela*. La Corte dijo en la sentencia SU-256/96: "En consecuencia, si, consideradas las circunstancias del caso, el accionante tiene la posibilidad de intentar la acción ordinaria enderezada a la indemnización de los daños que se le han causado, no es la tutela el medio judicial idóneo para ellos, pese a

[30] FLÓREZ RUIZ, Rodrigo. La protección de la intimidad económica con relación al dato financiero en la jurisprudencia constitucional colombiana (1992-2008), Universidad Autónoma Latinoamericana. Medellín, 2011, p 93.-95.

haber prosperado". Por lo tanto, el proceso ordinario civil es el camino procesal para reclamar los perjuicios que se desprendan por la violación de derechos fundamentales, por regla general.

- *La excepción, entonces, es la condena de los perjuicios en sede de tutela, lo cual es procedente conforme al artículo 25 del decreto 2591 de 1991*. La Corte, en diversas providencias, más antiguas que recientes, ha condenado al pago de perjuicios en sede de tutela en caso de mal manejo de la información financiera y de las mismas se desprende lo siguiente: a) En sede de tutela sólo puede condenarse al pago del daño emergente, no al pago del lucro cesante. B) Se puede condenar al pago de perjuicios morales por cuanto estos hacen parte del daño emergente. C) Sólo procede la condena si ésta es necesaria para posibilitar el goce de los derechos fundamentales vulnerados. D) La condena al pago de perjuicios en sede de tutela es *in genere.* E) La condena en abstracto se concreta en una liquidación que se hace por vía incidental ante la jurisdicción contencioso-administrativa, si es entidad pública, o ante el juez civil competente, si es entidad privada. El término de prescripción de la acción para liquidar los perjuicios ordenados en sede de Tutela es de seis meses. F) Los demás perjuicios causados se discuten y hacen efectivos por medio de las acciones ordinarias. G) En la vía incidental no se discute la existencia del daño que fue declarado en sede de tutela, simplemente se liquida el quantum del impacto económico, H) Los perjuicios morales los determina el juez según su arbitrio, teniendo en cuenta las circunstancias del caso. Esta sublínea jurisprudencial se ha desarrollado con relación al dato financiero, crediticio, comercial y de servicios a través de las sentencias T-257/02, T-575/96, SU-256/96, T-449/94, T-303/93, C-543/92."[31]

En conclusión todos los principios son importantes para crear un panorama general de cómo se debe efectuar el tratamiento y/o administración de los datos personales de las personas, pero se deben resaltar principalmente el principio de finalidad y el principio de libertad. Esto debido a que sobre estos dos principios se

[31]FLÓREZ RUIZ, Op. Cit., p. 95.

estructura el núcleo, el corazón, el alma de la administración de datos personales, ya que refiriéndonos al principio de libertad sólo se puede manipular los datos mediante la autorización previa, expresa e informada del titular de lo contrario todo tratamiento sería ilícito. Por otro lado, el principio de finalidad impone que única y exclusivamente se puede tratar la información acorde a la finalidad que se le informa al titular, de tal manera que otro trato divergente del informado al titular sería un trato ilícito. Lo que demuestra el por qué estos dos principios son de vital importancia y trascendencia a la hora de tratar datos personales.

5. DERECHOS INVOLUCRADOS EN LA PROTECCIÓN DE DATOS

En este numeral resulta importante destacar que el derecho al habeas data involucra a su interior varios derechos, pues de un lado están aquellos que buscan revelar la información de los titulares, como sería el derecho a la información, y de otro están los que buscan todo lo contrario, como el derecho a la intimidad. Lo anterior, debido a que hay ciertos datos que interesan a la sociedad, por ejemplo el historial crediticio de la persona, este dato es importante para determinar si el titular es sujeto de crédito o no. Así entonces se explica a continuación cada uno de estos derechos.

5.1 DERECHO A LA INTIMIDAD

La Constitución de 1991, tuvo presente la importancia y trascendencia de la información y su regulación para proteger los derechos fundamentales y evitar su vulneración, de tal manera que dispuso: "*Art 15: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar…".*

La protección de este derecho se sustenta en cinco principios de la protección de datos:

El principio de libertad, según el cual, los datos personales de un individuo, sólo pueden ser registrados o divulgados con el consentimiento libre, previo, expreso o tácito del titular, a menos que el ordenamiento jurídico le imponga la obligación de relevar dicha información, en aras de cumplir un objetivo constitucionalmente legítimo. En este contexto, la obtención y divulgación de datos personales, sin la previa autorización del titular o en ausencia de un claro y preciso mandato legal, se consideran ilícitas. El principio de finalidad, el cual se expresa en la exigencia de someter la recopilación y divulgación de datos, a la realización de una finalidad

constitucionalmente legítima, lo que impide obligar a los ciudadanos a relevar datos íntimos de su vida personal, sin un soporte en el Texto Constitucional que, por ejemplo, legitime la cesión de parte de su interioridad en beneficio de la comunidad. De conformidad con el principio de necesidad, la información personal que deba ser objeto de divulgación, se limita estrechamente a aquella que guarda relación de conexidad con la finalidad pretendida mediante su revelación. Así, queda prohibido el registro y la divulgación de datos que excedan el fin constitucionalmente legítimo. Adicionalmente, el principio de veracidad, exige que los datos personales que se puedan divulgar correspondan a situaciones reales y, por lo mismo, se encuentra prohibida la divulgación de datos falsos o erróneos. Por último, el principio de integridad, según el cual, la información que sea objeto de divulgación debe suministrarse de manera completa, impidiendo que se registre y divulgue datos parciales, incompletos o fraccionados.[32] El núcleo esencial del derecho a la intimidad, supone la existencia y goce de una órbita reservada en cada persona, exenta del poder de intervención del Estado o de las intromisiones arbitrarias de la sociedad, que le permita a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural.[33]

Para determinar cuándo una información deja de ser intima la Corte Constitucional en Sentencia T-787 de 2004 Dispuso:

> …Por consiguiente, una primera conclusión al estudio de la intimidad, permite fijar la siguiente regla: salvo las excepciones previstas en la Constitución y la ley, que obliguen a las personas a revelar cierta información a partir de su reconocimiento o valoración como de importancia o relevancia pública; el resto de los datos que correspondan al dominio personal de un sujeto no pueden ser divulgados, a menos que el mismo individuo decida revelar autónomamente su acceso al público…

[32] Ibid, sentencia T-787 de 2004, M.P. Rodrigo Escobar Gil
[33] Ibid, sentencia C-913 de 2010

Es vital darle la importancia que se merece a lo anterior, debido a que aún en la actualidad hay personas que tienen la conciencia de que la Ley 1266 de 2008 reguló el derecho a la intimidad, cuando esa afirmación es totalmente falsa, pues la información e historial crediticio de las personas no es información íntima ya que dichos datos tiene una importancia o relevancia pública. Resulta evidente que cuando una persona va a otorgar crédito o préstamo lo primero que quiere saber es su historial o información crediticia, así pues esta información es trascendental para el desarrollo de la actividad comercial, financiera, crediticia y de servicios de la sociedad.

5.2 DERECHO AL BUEN NOMBRE

La Constitución de Colombia de 1991 dispone: "*Art 15: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar…".*

Este derecho, ha sido definido por la Corte Constitucional como la reputación que acerca de una persona tienen los demás miembros de la sociedad en el medio en el cual éste se desenvuelve. El buen nombre es *un derecho típicamente proyectivo*, que supone la constante valoración a través del tiempo de la conducta del individuo, a partir de las acciones realizadas en su esfera de convivencia. El derecho al bueno nombre, es una valoración individual y colectiva que tiene su origen en todos los actos y hechos que una persona realice, para que, a través de ellos, la comunidad realice un juicio de valor sobre su comportamiento. La Corte también ha dicho que es buen nombre no es sólo un derecho proyectivo, sino también *derecho de valor*, es decir, su órbita de protección depende del adecuado comportamiento del individuo dentro de la sociedad, la cual califica su conducta como intachable y, por ende, merecedora de aceptación social. El buen nombre no se refiere únicamente al concepto que se tenga de una persona, sino también a la "buena imagen" que esta genera ante la sociedad. En este orden de ideas, esta corporación ha dicho que el citado derecho es vulnerado, cuando: "sin justificación

ni causa cierta y real, es decir, sin fundamento, se propagan entre el público, bien en forma o directa o personal, ya a través de los medios de comunicación informaciones falsas o erróneas o especies que distorsionan el concepto público que se tiene del individuo y que, por lo tanto, tienden a socavar el prestigio y la confianza de los que disfruta en el entorno social en cuyo medio actúa, o cuando en cualquier forma se manipula la opinión general para desdibujar su imagen".[34]

5.3 DERECHO A LA INFORMACIÓN

En el artículo 20 de la Constitución Colombiana se encuentra: *"Se garantiza a toda persona la libertad… de informar y recibir información veraz e imparcial, y de fundar medios masivos de comunicación…"*

El derecho a la información implica la posibilidad de recibir, buscar, investigar, almacenar, procesar, sistematizar, analizar, clasificar y difundir informaciones, concepto éste genérico que cubre tanto las noticias de interés para la totalidad del conglomerado como los informes científicos, técnicos, académicos, deportivos o de cualquier otra índole y los datos almacenados y procesados por archivos y centrales informáticas. El derecho a la información no es absoluto ni puede alegarse la garantía de su pleno disfrute como argumento para desconocer derechos de los asociados ni para evadir los necesarios controles estatales sobre la observancia del orden jurídico o sobre la prestación de los servicios que permitan canalizar informaciones al público. Por tanto, nada impide, a la luz de la Constitución, que el Estado contemple requisitos para recibir, manejar, difundir, distribuir o transmitir informaciones, ni que establezca restricciones o limitaciones por razón del imperio del orden jurídico, para hacer efectivos los derechos de las demás personas –tales como la honra, el buen nombre o la intimidad- o con el objeto de preservar el interés colectivo.[35]

[34] Ibid, sentencia T-787 de 2004, M.P. Rodrigo Escobar Gil
[35] Ibid, sentencia C-073 de 1996

Nótese entonces que este derecho puede entrar en colisión con otros como la intimidad y el bueno nombre, por ende es necesario establecer unos límites que deprenderán de la naturaleza que tengan los datos en cada caso concreto.

5.4 DERECHO A LA LIBERTAD DE EXPRESIÓN

La Constitución Nacional de Colombia en su artículo 20 indica: *"…Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones…"*

La libertad de expresión es una figura jurídica más amplia que la del derecho a la información. Abarca una generalidad que admite múltiples especies y, en virtud de la libertad de opinión y de pensamiento, no tiene tantas limitaciones como las que tienen el derecho a la información y el derecho de informar.[36] Se han distinguido ocho rasgos del ámbito constitucionalmente protegido de la libertad de expresión: (1) su titularidad es universal sin discriminación, compleja, y puede involucrar intereses públicos y colectivos, además de los intereses privados del emisor de la expresión; (2) sin perjuicio de la presunción de cobertura de toda forma de expresión por la libertad constitucional, existen ciertos tipos específicos de expresión prohibidos; (3) existen diferentes grados de protección constitucional de los distintos discursos amparados por la libertad de expresión, por lo cual hay tipos de discurso que reciben una protección más intensa que otros, lo cual a su vez tiene directa incidencia sobre la regulación estatal admisible y el estándar de control constitucional al que se han de sujetar las limitaciones; (4) protege expresiones exteriorizadas mediante el lenguaje convencional, como las manifestadas por medio de conducta simbólica o expresiva convencional o no convencional; (5) la expresión puede efectuarse a través de cualquier medio elegido por quien se expresa, teniendo en cuenta que cada medio en particular plantea sus propios problemas y especificidades jurídicamente relevantes, ya que la libertad constitucional protege tanto el contenido de la expresión como su forma

[36] Ibid, sentencia C-488 de 1993

y su manera de difusión; (6) la libertad constitucional protege tanto las expresiones socialmente aceptadas como aquellas consideradas inusuales, alternativas o diversas, lo cual incluye las expresiones ofensivas, chocantes, impactantes, indecentes, escandalosas, excéntricas o simplemente contrarias a las creencias y posturas mayoritarias, ya que la libertad constitucional protege tanto el contenido de la expresión como su tono; (7) su ejercicio conlleva, en todo caso, deberes y responsabilidades para quien se expresa; por último (8) impone claras obligaciones constitucionales a todas las autoridades del Estado, así como a los particulares.[37] A pesar de la presunción de que toda forma de expresión esta cobijada por el derecho fundamental en estudio existen ciertos tipos específicos de expresión prohibidos. Entre estos se cuentan: (a) la propaganda en favor de la guerra; (b) la apología del odio nacional, racial, religioso o de otro tipo de odio que constituya incitación a la discriminación, la hostilidad, la violencia contra cualquier persona o grupo de personas por cualquier motivo (modo de expresión que cobija las categorías conocidas comúnmente como discurso del odio, discurso discriminatorio, apología del delito y apología de la violencia); (c) la pornografía infantil; y (d) la incitación directa y pública a cometer genocidio. Estas cuatro categorías se han de interpretar con estricta sujeción a las definiciones fijadas en los instrumentos jurídicos correspondientes, para así minimizar el riesgo de que se sancionen formas de expresión legítimamente acreedoras de la protección constitucional. Con excepción de estas formas de expresión, estrictamente definidas, la presunción constitucional de cobertura por la libertad de expresión, y la sospecha correlativa de inconstitucionalidad de toda limitación –legislativa, administrativa o judicial- a la expresión, se aplican en principio a toda forma de expresión humana.[38]

[37] Ibid, sentencia C.442 de 2011
[38] Ibid, sentencia C.442 de 2011

5.5 SOLUCION DE CONFLICTOS

En la protección constitucional del derecho al habeas data, se pueden presentar ciertos problemas de relevancia constitucional cuando interactúa con otros derechos fundamentales como, por ejemplo, el derecho a la información previsto por el artículo 20 de la Constitución, según el cual se garantiza a todas las personas la libertad de informar y recibir información veraz e imparcial.[39] Lo anterior resulta obvio, debido a que por un lado está el derecho al habeas data, la intimidad y el buen nombre; y del otro, la información y el libre desarrollo de la personalidad que pueden llegar a verse inmersos en conflictos, ya sea a la hora de legislar en torno a éstos, ya sea poniéndoles limites o llenándolos de contenido donde se tendrá que tener en cuenta el principio de proporcionalidad ó en un caso concreto donde se tendrá que analizar qué derecho se sobrepone en esa situación concreta haciendo una ponderación.

5.5.1 Principio de proporcionalidad

De acuerdo con la conocida definición de H.L. Hart, un caso puede ser catalogado como fácil, cuando es posible reconocer a primera vista, si el evento que se presenta es uno de los ejemplos previstos por la norma que debe aplicarse. Expresado de otra manera, el interprete se sitúa frente a un caso fácil, cuando puede determinarse *ab initio* y sin mayores vacilaciones, si la hipótesis de que se trata se encuadra dentro de la referencia semántica de la disposición jurídica relevante o si, por el contrario, está excluida de ésta. Podemos considerar los casos fáciles de derecho fundamental en el control de constitucionalidad de las leyes, a aquéllos en los cuales es patente *a priori* que la norma legislativa examinada se encuadra dentro del supuesto de hecho de una norma directamente estatuida o, por el contrario, es evidente que se trata de una hipótesis excluida del mismo. Además de esto, para que un caso de derecho fundamental pueda ser

[39] Ibid, sentencia T-846 de 2004, M.P. Alfredo Beltrán Sierra

considerado como fácil, es necesario que no sean relevantes otros principios constitucionales que jueguen en contra de la relación a priori entre la norma directamente estatuida y la norma legislativa examinada.[40]

La situación anterior no se presenta en los casos difíciles, es decir, aquellos en los cuales, por causa de la indeterminación normativa de la disposiciones de derecho fundamental aplicable, no aparece claro *a priori* si la ley que se controla es compatible o incompatible con la norma de derecho fundamental directamente estatuida que resulta relevante. Dado que la norma directamente estatuida no basta para determinar la constitucionalidad o inconstitucionalidad de la ley, en estos casos es necesario concretar y fundamentar una nueva norma que sea adecuada para desempeñar la función de premisa mayor de la fundamentación interna de la sentencia. Esta nueva norma es una norma adscrita de derecho fundamental, que resuelve la situación de incertidumbre acerca de la constitucionalidad de la ley. La principal característica de estos tipos consiste en que en ellos se presenta un conflicto de argumentos constitucionales que juegan a favor y en contra de la declaración de inconstitucionalidad de la norma legal examinada. Este conflicto entre argumentos se soluciona mediante la concreción y la fundamentación de una norma adscrita de derecho fundamental.[41]

Resulta importante lo anterior, debido a que el legislador es quien determina el campo de acción de un derecho, es decir, éste le impone límites y lo llena de contenido junto con la Corte Constitucional. Es evidente que en algunos casos la ley deja vacíos o incertidumbre respecto a si cierta situación hace parte o no del supuesto que regula el derecho, lo que hace que el legislador vuelva nuevamente a expedir una norma para llenar dicho vacío. Así pues este principio de proporcionalidad lo que permite es brindar al legislador una herramienta para limitar o restringir un derecho.

[40] BERNAL PULIDO, Carlos. El principio de proporcionalidad y los derechos fundamentales, Centro de Estudios Políticos y Constitucionales. Madrid, 2003, p. 134-135
[41] Ibid, p. 141-143

Subprincipios de la proporcionalidad

El principio de proporcionalidad aparece como un conjunto articulado de tres subprincipios: idoneidad, necesidad y proporcionalidad en sentido estricto. Cada uno de esto subprincipios expresa una exigencia que toda intervención en los derechos fundamentales debe cumplir. Tales exigencias pueden ser enunciadas de la siguiente manera:

- Según el principio de idoneidad, toda intervención en los derechos fundamentales debe ser adecuada para contribuir a la obtención de un fin constitucionalmente legítimo.

- De acuerdo con el subprincipio de necesidad, toda medida de intervención en los derechos fundamentales debe ser la más benigna con el derecho intervenido, entre toras aquéllas que revisten por lo menos la misma idoneidad para contribuir a alcanzar el objetivo propuesto.

- En fin, conforme al principio de proporcionalidad en sentido estricto, la importancia de los objetivos perseguidos por toda intervención en los derechos fundamentales debe guardar una adecuada relación con el significado del derecho intervenido. En otros términos, las ventajas que se obtienen mediante la intervención en el derecho fundamental deben compensar los sacrificios que ésta implica para sus titulares y para la sociedad en general.[42]

5.5.2 La ponderación

Este principio cobra relevancia cuando hay un conflicto entre dos derechos, y se debe realizar un análisis, para la prevalencia de uno sobre otro. Esto es un juicio en donde se realza la subjetividad, pues ¿cómo se puede saber que un derecho tiene mayor peso que otro?

[42] Ibid, p. 35-36

Así, la Corte Constitucional ha dicho que, en el caso de colisión entre derechos constitucionales, corresponde al juez llevar a cabo la respectiva ponderación. Mediante ésta, se busca un equilibrio práctico entre las necesidades de los titulares de los derechos enfrentados. La consagración positiva del deber de respetar los derechos ajenos y no abusar de los propios, elevó a rango constitucional la auto-contención de la persona en el ejercicio de sus derechos. La eficacia constitucional de este deber, en consecuencia, exige de los sujetos jurídicos un ejercicio responsable, razonable y reflexivo de sus derechos, atendiendo a los derechos y necesidades de las demás y de la colectividad[43]

Entonces el proceso de ponderar significa asignarle un peso determinado a cada principio en el caso concreto, pues si no se realizara dicho procedimiento, ¿Cómo se solucionarían las colisiones entre principios de derechos fundamentales consagrados positivamente en una constitución? Entraríamos en una indeterminación normativa o en este caso una indeterminación de principios.[44]

Ahora, con el derecho al habeas data, en muchos casos hay dos derechos fundamentales que entran en colisión y estos son, el derecho a la intimidad y el derecho a la información, que según la Honorable Corte Constitucional en sentencia T-439/09 establece que, la protección de la propia imagen, junto con la de la intimidad y el honor, hacen parte de los llamados derechos personalísimos. Estos poseen autonomía propia, lo cual no significa que en ciertas situaciones no pueda verse menoscabados por medio de la violación del derecho de cada individuo a su imagen, que comprende la facultad de disponer de su apariencia y de su privacidad, autorizando o no su captación y su difusión. Todos los habitantes del territorio nacional tienen la libertad de publicar sus ideas sin censura previa; no obstante, esta libertad está limitada por la Constitución y las leyes que reglamentan su ejercicio. Ahora, si bien no puede restringirse la libertad de prensa,

[43] CORTE CONSTITUCIONAL. Sentencia T-425-95, M. P. Dr. Eduardo Cifuentes Muñoz.
[44] UNIVERSIDAD LIBRE. La ponderación y los derechos fundamentales, el modelo ponderativo de aplicación del derecho y su recepción en la Corte Constitucional Colombiana. Cartagena: Centro de investigaciones, 2011.

y tampoco puede someterse la difusión de ideas o informaciones a censura previa, sí puede el juez constitucional impedir la violación de los derechos al buen nombre y a la honra de la persona, ya sea por la prensa, por la televisión o por cualquier otro medio, como acto abusivo que no puede ser objeto de garantía constitucional. Cuando se prohíbe e impide la publicación o difusión de informaciones, noticias o imágenes que afectan la intimidad de la vida privada de la persona o de su buen nombre, no se está censurando una publicación o información que puede eventualmente ser difamatoria, calumniosa o injuriosa. Por el contrario, se está garantizando, de conformidad con lo dispuesto en el artículo 2º de la Constitución, la efectividad de los derechos de las personas que se pueden ver lesionadas por el contenido de la publicación, cuando éste resulte contrario a la verdad. Corresponderá entonces, al juez constitucional, en cada caso particular, en aras de asegurar la efectividad de los derechos fundamentales, evaluar si la información, imagen o noticia a la que se pretende dar difusión o la circulación de la publicación que contiene la revelación de hechos o situaciones íntimas han sido obtenidas ilegalmente, o sin la debida certeza y constatación de la objetividad de la información publicada.[45]

En conclusión para saber cuál derecho prevalece sobre el otro, el juez debe realizar un análisis, debe ponderar, en cada caso concreto y así establecer el derecho prima sobre el otro. Es por lo anterior que la ponderación, es un mecanismo de solución de conflictos que es verdaderamente importante y que no puede dejarse a un lado cuando se estudia el habeas data.

[45] Ibid, sentencia T-439/09, M. P. Dr. Jorge Ignacio Pretelt Chaljub

6. LEY 1581 DE 2012 Y DECRETO 1377 DE 2013

Como ya se ha dicho, en la vida diaria de las personas tanto jurídicas como naturales se ha vuelto necesaria la regulación respecto de sus datos. Lo anterior debido a que la tecnología y los medios de comunicación han avanzado muy rápido en los últimos años y se han visto nuevas formas de lesionar los derechos fundamentales. Así entonces es perentorio regular estas nuevas situaciones tal como lo manifiesta la Corte Constitucional desde sus inicios en el año 1992: *"…A partir de la vigencia del art. 15 de la Carta del 91 y en desarrollo del mismo es indispensable la regulación integral del poder informático para poner coto a sus crecientes abusos. Así lo exige la adecuada protección de la libertad personal frente a los poderosos embates de las nuevas tecnologías. Y así lo ordenará esta Sala".*[46]

Nótese que a pesar de que ya existía una preocupación de un organismo como la Corte Constitucional, sólo hasta el año 2008 el legislador reguló parcialmente este poder con la ley 1266 de 2008, y posteriormente se regularía de manera más amplia con la ley 1581 de 2012.

El propósito de este apartado es dar a conocer los aspectos más relevantes y trascendentes de la ley 1581 de 2012 de tal forma que el lector conozca, entienda y tome una postura crítica respecto de éstas. Antes de pasar a la ley es importante saber los sistemas existentes a nivel global para la protección de datos.

6.1 SISTEMA DE PROTECCIÓN DE DATOS

En el mundo existen dos sistemas para la protección de datos personales, un modelo centralizado y un modelo sectorial.

[46] Ibid, sentencia T-414 de 1992, p. 18

El primer modelo, implementado en los países europeos y, con algunas modificaciones, en la propia Unión Europea, parte de una categoría general de datos personales y de la idea de que cualquier tratamiento de ellos es considerado per se potencialmente problemático, razón por la cual debe sujetarse a unos principios y garantías mínimas comunes, susceptibles de ser complementadas con regulaciones especiales –según el tipo de dato y los intereses involucrados, pero que de ninguna manera suponen una derogación de los estándares de protección generales. Además, estos estándares generales, así como los especiales, son aplicables tanto al sector público como al privado. De lo anterior se puede entender que este sistema centralizado se enfoca por establecer unos parámetros generales para la protección de todos los datos personales que no pueden violarse aun cuando exista una norma especial que se relacione con una categoría de dato particular, es decir, que la norma general para la protección de datos personales es sólo y sólo una, y que a partir de ésta se pueden crear una protección especial dependiendo de la naturaleza del dato, pero siempre seguirán existiendo y siendo aplicable los patrones y mandatos generales. Por otro lado, está el sistema sectorial que no parte de una categoría común de datos personales y por ello no se ve necesario que todos los datos sean protegidos por una misma regulación mínima debido a que los datos son distintos, de tal manera que cada categoría de datos tendría su propia regulación y no existe un parámetro general común a todos. Este último sería el modelo implementado por Colombia hasta la entrada en vigencia de la Ley 1581 de 2012, pues nuestro país antes tenía por cada categoría especial de datos una norma específica y sectorial de regulación así por ejemplo está la Ley 1266 de 2008 que regula los datos que tengan la naturaleza de ser, información financiera y crediticia, comercial, de servicios y la proveniente de terceros países. También está la Ley 23 de 1981 “Por la cual se dictan normas en materia de ética médica”, cuyo artículo 34 dispone que la historia clínica “[e]s un documento privado sometido a reserva que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley” ”, y la Ley 96 de 1985, cuyo artículo 51 reconoce la

naturaleza pública de los datos sobre número de identificación personal y lugar y fecha de expedición, pero otorga carácter reservado a los archivos que reposan en la Registraduria ligados a la identificación, como datos biográficos, filiación y fórmula dactiloscópica. Así pues resulta evidente como en nuestra legislación se ha regulado el tema de manera sectorial y por ende que se haya acogido un sistema de protección de la misma naturaleza.

Es importante resaltar que con la Ley 1581 de 2012 se regula de manera íntegra todos los datos personales, es decir, que ya habría un parámetro y una base común para la protección de datos personales salvo que estos se vean regulados por una Ley especial, y en todo caso se les seguiría aplicando los principios de la Ley 1581, con lo que se adquiere también un modelo centralizado de protección de datos personales. En conclusión en Colombia actualmente existe un sistema híbrido de protección de datos personales debido a que convergen en el tema normas sectoriales por un lado y por otro lado están normas generales y comunes a la protección de datos.

6.2 ASPECTOS GENERALES DE LA LEY Y SU DECRETO

En este numeral se hablará de los aspectos generales de ley y su decreto, no se entrará analizar en su totalidad, pues se considera que se debe resaltar y profundizar en los temas que se tratan a continuación. Lo anterior debido a que éstos se preocupan y se enfocan más en demostrar lo que debe conocer todo el público en general y más concretamente los titulares de información que potencialmente puede ser toda la población, ya que de todos se pueden extraer datos personales.

6.2.1 Objeto

Es de gran importancia resaltar que la Ley 1581 de 2012 más conocida como la Ley de Protección de Datos Personales, tiene un objeto y margen de aplicación totalmente distinto a la Ley 1266 de 2008 y otras que regulen el derecho al Habeas Data. Si bien ambas normas desarrollan los derechos consagrados en los Artículos 15 y 20 de la Constitución Política Colombiana, la Ley 1266 es de carácter sectorial, pues limita su objeto a unos datos específicos y la Ley 1581 se concentra íntegramente en todos los datos que no sean objeto de una Ley especial, tal como lo dice la Corte Constitucional en la Sentencia C-748 de 2011, que examina la Constitucionalidad de la Ley 1581 de 2012:

> …En el caso colombiano, el proyecto de ley que dio lugar a la Ley 1266 de 2008 buscaba convertirse en una ley de principios generales aplicable a todas las categorías de datos personales. Sin embargo, como observó esta Corporación en la sentencia C-1011 de 2008, pese a su pretensión de generalidad, el proyecto de ley en realidad solamente establecía estándares básicos de protección para el dato financiero y comercial destinado a calcular el nivel de riesgo crediticio de las personas. Por ello en la referida sentencia, la Corte dejó claro que la materia de lo que luego se convertiría en la Ley 1266 es solamente el dato financiero y comercial. Por tanto, la Ley 1266 solamente puede ser considerada una regulación sectorial del habeas data.
>
> Este nuevo proyecto de ley busca llenar el vacío de estándares mínimos de protección de todos los datos personales –anunciado por la Corte Constitucional en la sentencia C-1011 de 2008, de ahí que su título sea precisamente “Por el cual se dictan disposiciones generales para la protección de datos personales”. Esa intención también fue anunciada por el gobierno en la exposición de motivos, en la que afirmó: “(…) es necesario que el país cuente con una legislación integral y transversal que garantice la protección efectiva de los datos personales en todo el proceso de tratamiento”. Como se verá más adelante, pese a varias deficiencias que presenta el proyecto, puede concluirse que efectivamente introduce principios y reglas generales destinadas a garantizar algunos contenidos mínimos del derecho al habeas data, entendido de la forma como se expuso previamente… (Negrillas fuera de texto original).

Esta Ley 1581 de 2012 tiene un gran impacto en la sociedad colombiana, ya que regula íntegramente el derecho al habeas data, acoge todos los datos que no estén regulados por normas especiales, y por ende como lo dice el objeto de la Ley tiene incidencia directa con varios derechos fundamentales, por un lado los derechos consagrados en el artículo 15 superior, que son el buen nombre, la intimidad y el habeas data ; De otro lado está el derecho a la información y a la libertad de expresión consagrados en el artículo 20 ibídem.

6.2.2 Ámbito de aplicación

La Ley 1581 de 2012 aplica a las bases de datos que no sean reguladas por una ley especial y que reúnan las siguientes tres condiciones acorde a su artículo 2: (i) la existencia de datos personales (ii) registrados en una base de datos que los haga susceptibles de tratamiento (iii) por entidades públicas o privadas. Es muy importante tener presente que también los archivos hacen parte del objeto de regulación de esta Ley, pues estos son depósitos ordenados de datos, incluidos datos personales, y suponen, como mínimo, que los datos han sido *recolectados, almacenados* y, eventualmente, *usados* –modalidades de tratamiento, son una especie de base de datos que contiene datos personales susceptibles de ser tratados y, en consecuencia, serán cobijados por esta ley.[47]

Respecto al tercer requisito al hablar de entidades, también debe entenderse por éstas a las personas naturales, ya que acorde al Diccionario de la Real Academia de la Lengua, una *entidad* puede ser un *"ente o ser"*; esta definición cobija a las personas naturales. De tal manera que el término *entidades* comprende tanto las personas naturales como las jurídicas.[48]

Por otro lado, el Artículo 2 establece explícitamente unas excepciones a las cuales no se le será aplicable la ley 1581 de 2012, éste indica:

[47] Ibid, sentencia C-748 de 2011, p. 91
[48] Ibid, sentencia C-748 de 2011, p. 91

> El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:
>
> a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
>
> Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley;
>
> b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;
>
> c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;
>
> d) A las bases de datos y archivos de información periodística y otros contenidos editoriales;
>
> e) A las bases de datos y archivos regulados por la Ley 1266 de 2008;
>
> f) A las bases de datos y archivos regulados por la Ley 79 de 1993.
>
> Parágrafo. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley (Subrayado propio).

Así pues, este artículo indica que bases de datos a pesar de cumplir con los requisitos anteriormente señalados no hacen parte del ámbito de aplicación de esta ley, ya sea porque tienen una ley sectorial como la ley 1266 de 2008 o porque dichos datos merecen un tratamiento distinto. Es importante resaltar que si bien a estas bases de datos no se les aplica esta ley, por disposición del parágrafo del artículo 2 si se le aplicarán los principios contenidos en misma, de tal forma que si bien no las cobija totalmente la ley, se puede considerar que si lo hace de manera parcial, ya que los principios representan un pilar fundamental en el tratamiento de

datos personales, tal como se ha demostrado anteriormente, especialmente el principio de libertad y el de finalidad.

6.3 DEFINICIONES

En las definiciones de la Ley 1266 de 2008 se nombran varias categorías de datos, como los privados, semiprivados y públicos, por qué en ésta no? La Corte Constitucional considera que la clasificación de los datos personales no es un elemento indispensable de la regulación y, dicho vacío en todo caso puede ser remediado acudiendo a la jurisprudencia constitucional y a otras definiciones legales, especialmente al artículo 3 de la Ley 1266, en virtud del principio de conservación del derecho.[49] De tal manera, que se puede acudir a la Ley 1266 u otras fuentes del derecho como lo es la jurisprudencia para categorizar los datos personales. A continuación se nombran y se explican las definiciones que trae la Ley 1581, con el objetivo de hacer más claro qué debe entenderse por cada una.

6.3.1 Base de datos

Frente a la definición de Base de Datos ya se explicó que también se entienden por éstas los archivos, por razones ya antes mencionadas. La Ley 1581 define la base de datos de la siguiente manera: “Conjunto organizado de datos personales que sea objeto de Tratamiento”.

6.3.2 Dato personal

Es trascendental la siguiente definición que hace el artículo 3 de la ley 1581 de 2012, para determinar qué Datos Personales regula la Ley: “*Dato personal:*

[49] Ibid, sentencia C-748 de 2011, p. 109

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables".

Aunque parezca que a partir del artículo anterior, esta ley no aplica para los datos personales de las personas jurídicas, ya que se entiende que sólo es dato personal aquel que *"pueda asociarse a una o varias personas naturales"* y por lo tanto se excluirían los datos de las personas jurídicas la Corte Constitucional en Sentencia C-748 de 2011 indica:

> …Por otra parte, llama la atención de la Sala que la definición del literal c) se restrinja a los datos de las personas naturales. Por tanto, la definición pareciera reñir, en principio, con algunos pronunciamientos de esta Corporación en los que se ha admitido que las personas jurídicas también pueden ser titulares del derecho al habeas data, como la sentencia T-462 de 1997 y C-1011 de 2008.
>
> Sin embargo, en sentir de la Sala, no se trata de una restricción que desconozca la doctrina constitucional sobre la protección del habeas data en cabeza de las personas jurídicas, ni el principio de igualdad. Ciertamente, la garantía del habeas data a las personas jurídicas no es una protección autónoma a dichos entes, sino una protección que surge en virtud de las personas naturales que las conforman. Por tanto, a juicio de la Sala, es legítima la referencia a las personas naturales, lo que no obsta para que, eventualmente, la protección se extienda a las personas jurídicas cuando se afecten los derechos de las personas que la conforman…

De tal manera que aunque se diga explícitamente que dato personal es aquel que puede asociarse a una o más personas naturales, la Corte ha dicho que el contenido de la norma, también puede extenderse a las personas jurídicas cuando se pueden ver vulnerados los derechos de las personas naturales que conforman a éstas. Por otro lado resulta trascendental para determinar más claramente qué es un dato personal regulado por la Ley volver a mirar la explicación que ya se hizo de dato personal, ya que hay datos personales públicos como el teléfono o la dirección los cuales gozan de una protección menos intensa que los datos personales de naturaleza privada, pero independiente de la naturaleza del dato que se trate, en ambos casos hay que pedir la autorización.

Habiendo dejado claro qué se entiende por dato personal, es menester indicar que existen unas categorías especiales de datos personales, entre éstas están:

6.3.3 Dato público

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.[50]

6.3.4 Datos sensibles

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.[51]

6.3.5 Datos de niños, niñas y adolescentes

El artículo 7 de la ley habla en particular de los datos pertenecientes a estos sujetos, pero en particular vale la pena resaltar que queda proscrito el Tratamiento

[50] Artículo 3, Decreto 1377 de 2013
[51] Ibid

de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.

El decreto 1377 de 2013 que reglamenta parcialmente esta ley impone como necesario para tratar este tipo de datos los siguientes requisitos:

> Artículo 12. Requisitos especiales para el tratamiento de datos personales de niños, niñas y adolescentes. El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7° de la Ley 1581 de 2012 y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos:
>
> 1. Que responda y respete el interés superior de los niños, niñas y adolescentes.
>
> 2. Que se asegure el respeto de sus derechos fundamentales.
>
> Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

6.3.6 Autorización

La autorización es el pilar fundamental de la administración de datos, pues ésta tiene relación directa con el principio de libertad y el derecho de autodeterminación informática que hace parte del núcleo esencial del derecho al habeas data. La Ley define la autorización como: *"Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales*".

Previo consentimiento quiere decir que la autorización debe ser suministrada, en una etapa anterior a la incorporación del dato. El derecho al *habeas data* resulta afectado cuando los administradores de la información recogen y divulgan hábitos de pago sin el consentimiento de su titular. La Corte expresó que el consentimiento previo del titular de la información sobre el registro de sus datos económicos "en los procesos informáticos, aunado a la necesidad de que aquel cuente con oportunidades reales para ejercer sus facultades de rectificación y

actualización durante las diversas etapas de dicho proceso, resultan esenciales para salvaguardar su derecho a la autodeterminación informática"[52]. Aunque la anterior explicación se enfoca en la información y datos económicos de la persona hay que entender que la autorización previa también es requisito indispensable en el tratamiento de los datos personas no relacionados con el carácter o comportamiento económico de las personas.

La autorización expresa quiere decir que ésta debe ser inequívoca, de tal manera que no puede aceptarse un consentimiento tácito. La jurisprudencia constitucional ha exigido tal condición y ha dicho que el consentimiento debe ser explícito y concreto a la finalidad específica de la base de datos. Por otro lado, la Ley indica que la autorización sea "obtenida por cualquier medio que pueda ser objeto de consulta posterior" lo que evidencia el por qué debe ser expresa la misma.

Finalmente, el carácter informado de la autorización quiere decir que el titular no sólo debe aceptar el Tratamiento del dato, sino también tiene que estar plenamente consciente de los efectos de su autorización.[53]

Acorde a todas estas características de la autorización no se permiten autorizaciones tácitas y el silencio del titular tampoco puede entenderse como autorización, y ésta debe ser previa, expresa e informada en todos los casos, para así cumplir con los requisitos legales y no tratar de manera ilícita la información.

También es importante resaltar que al momento de pedir la autorización la ley 1581 de 2012 le impone al responsable del tratamiento la obligación de informarle de manera clara y expresa al titular lo siguiente:

a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;

[52] Ibid, sentencia C-748 de 2011, p. 129
[53] Ibid, sentencia C-748 de 2011, p. 129

b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;

c) Los derechos que le asisten como Titular;

d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.[54]

¿Cuándo no es necesaria la autorización?

Por otro lado, es importante indicar que no es necesaria la autorización en todos los casos, pues existen unas excepciones tal como lo indica el artículo 10 de la ley, éstas son:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;

b) Datos de naturaleza pública;

c) Casos de urgencia médica o sanitaria;

d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;

e) Datos relacionados con el Registro Civil de las Personas

¿Cómo pedir la autorización?

Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca. (Artículo 7 del

[54] Artículo 12 de la ley 1581 de 2012

decreto). Como consecuencia de lo anterior los responsables deben conservar prueba de la autorización por parte del titular, tal como lo indica el artículo 8 del decreto.

¿Cuándo pedir la autorización?

El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento.(Artículo 5 del decreto).

Respecto a lo anterior surge el siguiente interrogante: ¿Qué pasa con los datos de los titulares que ya han sido recogidos con anterioridad a esta ley y decreto y por ende que no cumplen con esta obligación?

El artículo 10 del decreto indica:

> Para los datos recolectados antes de la expedición del presente decreto, se tendrá en cuenta lo siguiente:
>
> 1. Los responsables deberán solicitar la autorización de los titulares para continuar con el Tratamiento de sus datos personales del modo previsto en el artículo 7° anterior, a través de mecanismos eficientes de comunicación, así como poner en conocimiento de estos sus políticas de Tratamiento de la información y el modo de ejercer sus derechos.
>
> 2. Para efectos de lo dispuesto en el numeral 1, se considerarán como mecanismos eficientes de comunicación aquellos que el responsable o encargado usan en el curso ordinario de su interacción con los Titulares registrados en sus bases de datos.
>
> 3. Si los mecanismos citados en el numeral 1 imponen al responsable una carga desproporcionada o es imposible solicitar a cada Titular el consentimiento para el Tratamiento de sus datos personales y poner en su conocimiento las políticas de Tratamiento de la información y el modo de ejercer sus derechos, el Responsable podrá implementar mecanismos alternos para los efectos dispuestos en el numeral 1, tales como diarios de amplia circulación nacional, diarios locales o revistas, páginas de Internet del responsable, carteles informativos, entre otros, e informar al respecto a la

Superintendencia de Industria y Comercio, dentro de los cinco (5) días siguientes a su implementación.

Con el fin de establecer cuándo existe una carga desproporcionada para el responsable se tendrá en cuenta su capacidad económica, el número de titulares, la antigüedad de los datos, el ámbito territorial y sectorial de operación del responsable y el mecanismo alterno do comunicación a utilizar, de manera que el hecho de solicitar el consentimiento a cada uno de los Titulares implique un costo excesivo y que ello comprometa la estabilidad financiera del responsable, la realización de actividades propias de su negocio o la viabilidad de su presupuesto programado.

A su vez, se considerará que existe una imposibilidad de solicitar a cada titular el consentimiento para el Tratamiento de sus datos personales y poner en su conocimiento las políticas de Tratamiento de la información y el modo de ejercer sus derechos cuando el responsable no cuente con datos de contacto de los titulares, ya sea porque los mismos no obran en sus archivos, registros o bases de datos, o bien, porque estos se encuentran desactualizados, incorrectos, incompletos o inexactos.

4. Si en el término de treinta (30) días hábiles, contado a partir de la implementación de cualesquiera de los mecanismos de comunicación descritos en los numerales 1, 2 y 3, el Titular no ha contactado al Responsable o Encargado para solicitar la supresión de sus datos personales en los términos del presente decreto, el responsable y encargado podrán continuar realizando el Tratamiento de los datos contenidos en sus bases de datos para la finalidad o finalidades indicadas en la política de Tratamiento de la información, puesta en conocimiento de los titulares mediante tales mecanismos, sin perjuicio de la facultad que tiene el Titular de ejercer en cualquier momento su derecho y pedir la eliminación del dato.

5. En todo caso el Responsable y el Encargado deben cumplir con todas las disposiciones aplicables de la Ley 1581 de 2012 y el presente decreto. Así mismo, será necesario que la finalidad o finalidades del Tratamiento vigentes sean iguales, análogas o compatibles con aquella o aquellas para las cuales se recabaron los datos personales inicialmente.

Parágrafo. La implementación de los mecanismos alternos de comunicación previstos en esta norma deberá realizarse a más tardar dentro del mes siguiente de la publicación del presente decreto (Subrayado Propio).

Lo anterior resulta trascendental para el tratamiento de datos personales, pues resulta que desde hace muchos años en el desarrollo de la vida diaria de las personas se solicitan datos como en el comercio, en el empleo, en un club social, colegio, etc. Estos datos pueden ser por ejemplo: número celular, número de hijos,

lugar de residencia, entre otros. Partiendo de lo anterior es obvio que antes de la ley y el decreto no se hubiera pedido autorización por lo cual es importante el artículo anterior y más concretamente lo subrayado. Nótese que el artículo exige que se pida autorización por los medios ordinarios por los cuales se comunican el titular y el responsable del tratamiento de datos, pero en algunas circunstancias esto puede resultar oneroso para el responsable o que éste no tenga como contactar al titular. En este caso el decreto permite implementar “medios alternativos” siempre y cuando se presente dicha implementación a más tardar dentro del mes siguiente de la publicación del decreto. Así entonces, el decreto fue publicado en el diario oficial el día 27 de junio de 2013, lo cual indica que se podía implementar medios alternativos hasta el 26 de julio de 2013 y quienes no hayan utilizado esta posibilidad sólo les queda comunicarse a través de otro medio y obtener la autorización del titular, si pasados 30 días a partir de dicha comunicación el titular no se manifiesta respecto a la autorización o su voluntad de que se elimine la información , el responsable podrá seguir utilizando la misma como lo venía haciendo según las finalidades establecidas en el manual de políticas del responsable.

Ahora bien, la ley 1581 de 2012 en su artículo 12 impone al responsable del tratamiento al momento de pedir la autorización el siguiente deber:

> Artículo 12. Deber de informar al Titular. El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:
>
> a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
>
> b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
>
> c) Los derechos que le asisten como Titular;
>
> d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

> Parágrafo. El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta.

Revocatoria de la Autorización

El Artículo 9 del Decreto nos indica que los titulares mediante la presentación de un reclamo pueden pedir en todo momento la supresión del dato o la revocatoria de la autorización, pero éste también indica que: "*La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos" (Negrilla propia).*

La anterior situación en negrilla se puede presentar en el caso que un trabajador de una empresa pida que se eliminen sus datos, pero no se efectuará dicho acto debido a que existe un vínculo contractual de trabajador que tiene con la empresa esta circunstancia lo lleva permanecer en la base de datos, por lo menos hasta que deje de existir dicha relación.

Ahora bien, si no hay obligación de permanecer en la base de datos y se vencen los términos legales para resolver el reclamo del titular de eliminar su información, éste puede solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales, siguiendo el trámite descrito en el Código Contencioso Administrativo.

Cambio de finalidad y una nueva autorización

Como se ha venido indicando la autorización que se pide al titular del dato va sujeta a la finalidad para la cual el responsable del tratamiento solicita los datos del titular, pero qué pasará si se cambia la finalidad, se requerirá de una nueva autorización? El artículo 5 del decreto nos indica: "*En caso de haber cambios sustanciales en el contenido de las políticas del Tratamiento a que se refiere el Capítulo III de este decreto, referidos a la identificación del Responsable y a la*

finalidad del Tratamiento de los datos personales……deberá obtener del Titular una nueva autorización cuando el cambio se refiera a la finalidad del Tratamiento" (Subrayado Propio).

Lo anterior, resulta obvio, pues la finalidad es el marco de acción dentro del cual se pueden tratar los datos, y si esta cambia se debe pedir una nueva autorización. Así mismo si se cumple la finalidad, es decir, si esta ya se alcanzó se deben eliminar los datos y dejar de tratarlos debido a que la finalidad resulta ser un límite de temporalidad al tratamiento.

Autorización y datos sensibles

Habiendo ya definido qué se entiende por datos sensibles, es menester indicar que el decreto exige unos requisitos adicionales a la hora de pedir la autorización al titular para tratar esta categoría de datos. El artículo 6 indica:

> En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo *6*° de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:
>
> 1. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.
>
> 2. Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.
>
> Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.

De tal forma, que cumpliendo los prescrito por este artículo se pueden tratar los datos sensibles.

A quien se le puede suministrar la información?

La anterior pregunta resulta trascendental, debido a que hoy en día se presenta una gran competencia por la información, hasta el punto que se convierte en una

mercancía y las personas tanto las naturales como las jurídicas compran y venden bases de datos. Un ejemplo de esto es el recibir correos electrónicos que contienen publicidad de empresas que muchas veces el titular del dato (correo electrónico) ni conoce o no recuerda haber dado su correo a dicha entidad o empresa. Así pues la ley 1581 de 2012 indica a quien se puede suministrar la información.

> Artículo 13. Personas a quienes se les puede suministrar la información. La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas:
>
> a) A los Titulares, sus causahabientes o sus representantes legales;
>
> b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;
>
> c) A los terceros autorizados por el Titular o por la ley.

Acorde a esto, se restringe esa compra y venta descontrolada que había de base de datos, y se aspira que los responsables y encargados del tratamiento cumplan lo anterior, ya que de no hacerlo podrán ser investigados y sancionados conforme a la ley.

6.3.7 Responsable del tratamiento y encargado del tratamiento

La Ley 1581, dentro de sus definiciones, nos indica lo siguiente:

> Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.
>
> Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

Las dos anteriores definiciones se prestan para confusiones, pues nacen preguntas como: ¿Pueden concurrir las dos calidades en una misma persona?

¿Cómo determinar quién es el responsable y quién es el Encargado?, entre otras. En respuesta a lo anterior, y en aras de aclarar la confusión, la Corte Constitucional en la Sentencia C-748 de 2011 nos ilustra de una manera más clara, determinando qué debe entenderse por cada uno. En la Sentencia la Corte indica que estos conceptos parecen inspirarse en el derecho comunitario europeo especialmente en la Directiva 95/46/CE y en el Dictamen 1/2010 del Grupo Consultivo sobre Protección de Datos.

El Dictamen 1/2010 señala que lo que permite identificar al responsable de otros agentes que participan en el proceso, es que él es el que determina los fines y los medios esenciales del tratamiento de los datos. También indica en relación con los medios, que se hablará de responsable cuando el sujeto realice un control o determine elementos esenciales de los medios, tales como el tiempo que los datos deben permanecer almacenados, la forma cómo se hará su uso o se pondrán en circulación, el acceso a los mismos etc. Por su parte, precisa que el encargado es quien realiza el tratamiento por cuenta del responsable, es decir, por delegación y, por tanto, es natural y jurídicamente distinto del responsable. Ciertamente, el concepto *"decidir sobre el tratamiento"* empleado por el literal e) (responsable del tratamiento) parece coincidir con la posibilidad de definir –jurídica y materialmente- los fines y medios del tratamiento. Usualmente, como reconocen varias legislaciones, el responsable es el propietario de la base de datos; sin embargo, con el fin de no limitar la exigibilidad de las obligaciones que se desprenden del habeas data, la Sala observa que la definición del proyecto de ley es amplia y no se restringe a dicha hipótesis. Así, el concepto de responsable puede cobijar tanto a la fuente como al usuario (refiriéndose a las definiciones que hace la Ley 1266 de 2008), en los casos en los que dichos agentes tengan la posibilidad de decidir sobre las finalidades del tratamiento y los medios empleados para el efecto, por ejemplo, para ponerlo en circulación o usarlo de alguna manera.[55]

[55] Ibid, sentencia C-748 de 2011, p. 110 - 111

De otro lado, el criterio de delegación coincide con el término "*por cuenta de"* utilizado por el literal e), lo que da a entender una relación de subordinación del encargado al responsable, sin que ello implique que se exima de su responsabilidad frente al titular del dato. Así, por ejemplo, será responsable del dato el hospital que crea la historia clínica de su paciente, la universidad o las instituciones educativas en relación con los datos de sus alumnos, pues estos determinan la finalidad (en razón de su objeto que, puede estar señalado en una ley o por el giro normal de la actividad que desarrollan) para la recolección de los datos, así como la forma en que los datos serán procesados, almacenados, circulados, etc. [56]

Ahora bien, vale la pena advertir que el encargado del tratamiento no puede ser el mismo responsable, pues se requiere que existan dos personas identificables e independientes, natural y jurídicamente, entre las cuales una –el responsable- le señala a la otra -el encargado- como quiere el procesamiento de unos determinados datos. En este orden, el encargado recibe unas instrucciones sobre la forma como los datos serán administrados.

Volvamos al ejemplo de la historia clínica, en el que la institución de salud contrata con una compañía el procesamiento de las historias para que con un programa especial que puede determinar el responsable o la empresa contratada, le organice la información contenida en ellas, siguiendo las indicaciones que establece el hospital. En este caso, el encargado del tratamiento de los datos es la persona jurídica que elige contratar el hospital para el procesamiento de las hojas de vida. En efecto, de acuerdo con las definiciones acogidas por el proyecto de ley, los responsables del tratamiento tienen mayores compromisos y deberes frente al titular del dato, pues son los llamados a garantizar en primer lugar el derecho fundamental al habeas data, así como las condiciones de seguridad para impedir cualquier tratamiento ilícito del dato. La calidad de responsable igualmente

[56] Ibid, sentencia C-748 de 2011, p. 110 - 111

impone un haz de responsabilidades, específicamente en lo que se refiere a la seguridad y a la confidencialidad de los datos sujetos a tratamiento.[57]

Finalmente se debe mirar los artículos 17 y 18 de la ley 1581 de 2012 en aras de observar cuáles son los deberes del responsable y del encargado del tratamiento de datos personales.

6.3.8 Titular del dato

Frente a esta definición sólo basta indicar que a pesar de que la Ley indica que el titular del dato es la persona natural, también podrá extenderse esta calidad de titular a las personas jurídicas cuando existan datos personales que haya que proteger de las personas naturales que las conforman. Además hay que reiterar nuevamente que es el titular el único propietario del dato, como ya se dejó indicado anteriormente, ya que si bien el responsable y/o es el dueño de la base de datos, eso no los vuelve dueños de la información en ella contenida.

De otro lado, vale la pena resaltar los derechos que tiene el titular que son:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;

[57] Ibid, sentencia C-748 de 2011, p. 110 - 111

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.[58]

Habiendo dicho lo anterior es menester indicar quiénes pueden ejercer los derechos de los titulares, es decir, quiénes son los legitimados para ejercer los anteriores derechos enumerados anteriormente, para lo cual indica la ley 1581 de 2012:

Artículo 20. *Legitimación para el ejercicio de los derechos del titular.* Los derechos de los Titulares establecidos en la Ley, podrán ejercerse por las siguientes personas:

1. Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.

2. Por sus causahabientes, quienes deberán acreditar tal calidad.

3. Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.

[58] Artículo 8, ley 1581 de 2012

4. Por estipulación a favor de otro o para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos

6.3.9 Tratamiento

El vocablo tratamiento para los efectos de la ley 1581 de 2012 en análisis es de suma importancia por cuanto su contenido y desarrollo se refiere precisamente a lo que debe entenderse por el "*tratamiento del dato personal*". En ese orden, cuando la ley se refiere al tratamiento, hace alusión a cualquier operación que se pretenda hacer con el dato personal, con o sin ayuda de la informática, pues a diferencia de algunas legislaciones, la definición que aquí se analiza no se circunscribe únicamente a procedimientos automatizados. Es por ello que los principios, derechos, deberes y sanciones que contempla la normativa en revisión incluyen, entre otros, capturar, procesar, almacenar, custodiar, conservar, transferir, transmitir y en general usar información y otras formas de procesamiento de datos con o sin ayuda de la informática. En consecuencia, no es válido argumentar que la ley de protección de datos personales cobija exclusivamente el tratamiento de datos que emplean las nuevas tecnologías de la información, dejando por fuera las bases de datos manuales, lo que resultaría ilógico, puesto que precisamente lo que se pretende con este proyecto es que todas las operaciones o conjunto de operaciones con los datos personales quede regulada por las disposiciones del proyecto de ley en mención, con las salvedades.[59]

[59] Ibid, sentencia C-748 de 2011, p. 113

6.3.10 Políticas de tratamiento

El decreto 1377 de 2013 introduce como obligación de los responsables tener unas “políticas de tratamiento de datos personales” y velar por que los encargados las cumplan. Estas políticas se deben poner a disposición de los titulares y si no se pudiere se deberá hacer saber a los titulares de éstas a través de un aviso de privacidad.

El contenido de las políticas de tratamiento acorde al artículo 13 del decreto 1377 es el siguiente:

Las políticas de Tratamiento de la información deberán constar en medio físico o electrónicas, en un lenguaje claro y sencillo y ser puestas en conocimiento de los Titulares. Dichas políticas deberán incluir, por lo menos, la siguiente información:

1. Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.

2. Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad.

3. Derechos que le asisten como Titular.

4. Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.

5. Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.

6. Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.

El objeto de esta obligación de tener políticas de tratamiento de datos personales es garantizar una estructura en cada base de datos o archivos (como se dijo anteriormente), de tal forma que se haga un buen uso de los datos, y se respeten los derechos de los titulares y se le brinden herramientas para hacer valer estos últimos. Resulta importante tener estas políticas, pues resulta que anteriormente no existía al interior de las organizaciones un manual o esquema que orientara al titular para hacer valer sus derechos, surgían preguntas como ¿a quién llamo?, ¿qué procedimiento debo seguir?, ¿qué derechos tengo?, entre otras.

6.3.11 Aviso de privacidad

Este aviso resulta algo nuevo que trae el decreto 1377 y que no está en la ley 1581, el decreto lo define así: *"Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales."*[60]

Se parece un poco a la autorización, pues al parecer se podría omitir alguna de las dos, ya que en ambas se informa la finalidad para la cual serán usados los datos personales del titular, pero en realidad son dos cosas totalmente distintas, debido al que el contenido del aviso de la privacidad es el siguiente:

1. Nombre o razón social y datos de contacto del responsable del tratamiento.

2. El Tratamiento al cual serán sometidos los datos y la finalidad del mismo.

3. Los derechos que le asisten al titular.

[60] Artículo 3, decreto 1377 de 2013

4. Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.

Es importante adicionar que acorde al decreto 1377 cuando se recolecten datos sensibles, se debe señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.

En todo caso, la divulgación del Aviso de Privacidad no eximirá al Responsable de la obligación de dar a conocer a los titulares la política de tratamiento de la información.[61]

Nótese entonces que el aviso de privacidad si bien puede parecer una autorización es totalmente distinto a ésta, pues tiene un contenido más amplio que la segunda. Resulta importante resaltar que se puede omitir el aviso de privacidad si se da a conocer las "políticas de tratamiento" al titular, y que a nuestro juicio ocurre en la mayoría de los casos, pues resulta superfluo mandar un aviso de privacidad si de todas manera como dice la norma "*En todo caso, la divulgación del Aviso de Privacidad no eximirá al Responsable de la obligación de dar a conocer a los titulares la política de tratamiento de la información".* De tal forma para qué mandar un aviso de privacidad si de todas formar tengo que construir las políticas de tratamiento de datos personales y dárselas a conocer al titular, más fácil hacer de una vez la segunda, para así poder omitir el primero.

6.3.12 Autoridad de protección de datos personales

La autoridad competente para la protección de datos es la Superintendencia de Industria y Comercio, la cual dispondrá de un Superintendente Delegado para

[61] Artículo 15, decreto 1377 de 2013

ejercer las funciones de Autoridad de Protección de Datos. Actualmente quien ocupa el cargo es el Doctor José Alejandro Bermúdez Durana, y esta entidad para cumplir sus funciones se basa en los recursos que le dé el presupuesto nacional de la nación.

La misma ley, en el artículo 21 le otorga las funciones a la entidad encargada que son las siguientes:

a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;

b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;

c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva;

d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementará campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos;

e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley;

f) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.

g) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos;

h) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento;

i) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional;

j) Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personajes;

k) Las demás que le sean asignadas por ley.

Es la misma entidad, actuando a través del Superintendente Delegado, quien decretará las sanciones y tomará las medidas que considere oportunas. Lo no reglado en esta ley, o en sus decretos reglamentarios será tratado por las normas pertinentes del Código Contencioso Administrativo.

Es importante señalar que la Superintendencia de Industria y Comercio, solamente podrá imponer estas multas o sanciones, cuando el infractor sea una persona de naturaleza privada. Si el incumplimiento proviene de una autoridad pública, ésta entidad deberá remitir la actuación a la Procuraduría General de la Nación, para que sea quien adelante la investigación respectiva.

Las sanciones que puede establecer la Superintendencia de Industria y Comercio, a los Responsables del Tratamiento y Encargados del Tratamiento son, de acuerdo al artículo 23 de la ley, las siguientes:

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

Para sancionar y hacer valer lo anterior la SIC[62], tendrá en cuenta la dimensión del daño o peligro a los intereses jurídicos tutelados por la ley; El beneficio económico obtenido por el infractor o terceros; La reincidencia en la comisión de la infracción; La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la SIC; La renuencia o desacato a cumplir las órdenes impartidas por la SIC y El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

Así nótese que las sanciones pueden ir desde el pago de dinero hasta el cierre definitivo de la empresa, lo cual debería traer como consecuencia que los sujetos que manejan bases de datos objeto de esta ley cumplan todas las disposiciones en aras de evitar cualquier perjuicio o sanción en contra.

[62] Superintendencia de Industria y Comercio

6.4 MECANISMOS DE PROTECCIÓN

A continuación se hará énfasis en los mecanismos de protección que otorga la ley al titular de la información para hacer valer sus derechos y que por ende el tratamiento de los datos no se haga de manera ilícita.

Dentro de estos mecanismos encontramos los trámites de consulta y reclamos frente al responsable del tratamiento; y el trámite de queja ante la SIC.

Frente al trámite de consulta es menester indicar que el Titular o sus Causahabientes (en caso de muerte del primero) podrán consultar de forma gratuita los datos personales: (i) al menos una vez cada mes calendario, y (ii) cada vez que existan modificaciones sustanciales de las Políticas de Tratamiento de la información que motiven nuevas consultas. Para consultas cuya periodicidad sea mayor a una por cada mes calendario, el responsable solo podrá cobrar al titular los gastos de envío, reproducción y, en su caso, certificación de documentos.[63] Por otro lado, el artículo 14 de la ley 1581 de 2012 establece 10 días hábiles una vez recibida la consulta para solucionar, si no se puede cumplir con la obligación legal en ese término se tendrán otros 5 días hábiles siempre y cuando se le indique al titular las razones de la demora y que sea justificable el atraso.

Frente al trámite de reclamo la ley indica que el titular o su causahabiente debe acompañar con éste la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo. La ley indica que se tendrán 15 días hábiles para solucionar y otros 8 días hábiles en caso de no poder solucionar siempre y cuando se le indique al titular o a su causahabiente el motivo del retraso y se justifique.

[63] Artículo 21, Decreto 1377 de 2013

Es importante indicar que la ley establece unos términos específicos, pero en todo caso al interior de las entidades se pueden establecer términos menores, lo que sino se puede es establecer unos superiores.

Por otro lado está el trámite de queja ante la SIC, pero para acudir a éste la ley exige como requisito de procedibilidad que se haya agotado el trámite de reclamo ante el responsable del tratamiento.

7. CONCLUSIONES

Con el avance de la tecnología y la información, y la presencia de éstos cada vez más en el día a día de las personas el habeas data ha tomado gran protagonismo e importancia en los últimos tiempos, si bien toda en un principio su regulación era principalmente jurisprudencial a través de las sentencias de la Corte Constitucional, posteriormente fue regulado legalmente a través de la ley estatutaria 1266 de 2008 y más tarde de manera más amplia por la ley objeto de este trabajo, la 1581 de 2012 y su decreto 1377 de 2013. Conforme a este escrito no queda duda alguna de que el habeas data es un derecho fundamental y autónomo, pues si bien tiene relación con otros derechos como la intimidad y la información, se distingue de ellos totalmente ya que tiene un núcleo esencial distinto a éstos, tal y como quedo demostrado anteriormente.

De otro lado, es importante resaltar que este derecho al ser fundamental y autónomo es viable su protección a través de la acción de tutela. Frente a esto es menester indicar que si bien se puede presentar un conflicto entre este derecho y otros como la información o la intimidad, será el juez en cada caso concreto a través de herramientas como la ponderación quien decidirá qué derecho debe primar sobre el otro en dicha situación específica.

Además del mecanismo de la tutela, es relevante mencionar además otros mecanismos de protección que emanan directamente de la ley 1581 de 2012, estos son el trámite de consulta, el reclamo y la queja ante la SIC. Se consideran mecanismos de protección toda vez que a través de éstos el titular de la información puede ejercer su derecho al habeas data.

No se pretende con el trabajo abarcar con una gran profundidad el tema del derecho al habeas data, ni mucho menos abarcar todos los aspectos que componen a éste derecho, se busca dar un panorama general sobre en qué

consiste, cómo se administra y cómo se protege este derecho, objetivo que se considera que se cumplió.

Uno de los aspectos que no se tocó en el presente trabajo, es el de la transferencia y transmisión internacional de datas. Lo anterior por varias razones, una de ellas, como se dijo anteriormente, el presente escrito no buscaba abarcar la totalidad de los aspectos del derecho, simplemente se pretendía realizar un mapa general de la situación dentro de nuestro país, en segundo lugar, se piensa que es de mayor conveniencia para el lector conocer en un primer instante la legislación interna para después conocer cómo funciona el derecho del habeas data internacionalmente.

Es trascendental dejar claro que la ley no ha sido reglamentada en su totalidad, por ejemplo existen cosas pendientes como el “Registro Nacional de Bases de Datos” de que habla el artículo 25, que la define como el directorio público de las bases de datos sujetas a Tratamiento que operan en el país y que será operado por la SIC, pero en la actualidad no ha habido reglamentación y por ende aun no existe dicho registro nacional.

Finalmente, no se puede creer que este derecho ya está en su gran mayoría regulado y desarrollado, si bien es cierto que ya hay maneras efectivas para hacer que se respete, o para indemnizar los perjuicios causados cuando se viola, o para sancionar a aquellas personas o entidades que han hecho un mal uso de la información que protege este derecho, el habeas data es un derecho que sigue en constante evolución.

BIBLIOGRAFIA

- BERNAL PULIDO, Carlos. El principio de proporcionalidad y los derechos fundamentales, centro de estudios políticos y constitucionales. Madrid, 2003.
- CHINCHILLA, Tulio. ¿Qué son y cuáles son los derechos fundamentales? Segunda edición. Bogotá: Editorial Temis.
- CÓDIGO CONTENCIOSO ADMINISTRATIVO.
- COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581 de 2012: “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- -------- 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, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.
- -------- Ley 23 de 1981: “Por la cual se dictan normas en materia de ética médica”.
- -------- Ley 96 de 1985: “Por la cual se modifican las Leyes 28 de 1979 y 85 de 1981, el Código Contencioso Administrativo, se otorgan unas facultades extraordinarias y se dictan otras disposiciones”.
- COLOMBIA. CORTE CONSTITUCIONAL. Sentencia C-073 De 1996, M.P.: Dr. José Gregorio Hernández Galindo
- -------- Sentencia C-442 De 2011, M.P.: Humberto Antonio Sierra Porto
- -------- Sentencia C-488 De 1993, M.P.: Dr. Vladimiro Naranjo Mesa
- -------- Sentencia C-748 De 2011, M.P.: Jorge Ignacio Pretelt Chaljub.

- -------- Sentencia C-913 De 2010, M.P.: Nilson Pinilla Pinilla
- -------- Sentencia Su-082 De 1995, M.P.: Jorge Arango Mejía.
- -------- Sentencia T-067 Del 2007, M.P.: Rodrigo Escobar Gil
- -------- Sentencia T-094 De 1995, M.P.: Dr. José Gregorio Hernández Galindo
- -------- Sentencia T-176 De 1995, M.P.: Eduardo Cifuentes Muñoz
- -------- Sentencia T-414 De 1992, M.P.: Ciro Angarita Barón.
- -------- Sentencia T-425-95, M.P.: Dr. Eduardo Cifuentes Muñoz.
- -------- Sentencia T-439/09, M.P.: Dr. Jorge Ignacio Pretelt Chaljub
- -------- Sentencia T-658 De 2011, M.P.: Dr. Jorge Ignacio Pretelt Chaljub.
- -------- Sentencia T-787 De 2004, M.P.: Rodrigo Escobar Gil
- -------- Sentencia T-846 De 2004, M.P.: Alfredo Beltrán Sierra
- COLOMBIA. PRESIDENCIA DE LA REPUBLICA. Decreto 1377 de 2013: “Por el cual se reglamenta parcialmente la ley 1581 del 2012”.
- -------- Decreto 2591 de 1991: “Por el cual se reglamenta la acción de tutela consagrada en el artículo 86 de la Constitución Política”.
- FLÓREZ RUIZ, Rodrigo. La protección de la intimidad económica con relación al dato financiero en la jurisprudencia constitucional colombiana (1992-2008), Universidad Autónoma Latinoamericana. Medellín, 2011.
- PÉREZ LUÑO, Antonio. Los derechos fundamentales. Madrid: Tecnos, 1998.
- SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO.

- UNIVERSIDAD LIBRE. La ponderación y los derechos fundamentales, el modelo ponderativo de aplicación del derecho y su recepción en la Corte Constitucional Colombiana. Cartagena: Centro de investigaciones, 2011

- Http://blog.derecho-informatico.org/faqs/datos-personales/