La responsabilidad demostrada frente al tratamiento de datos personales y su relevancia para la graduación de la sanción al interior de procedimientos administrativos sancionatorios

Diego Fernando Montezuma Chavez

Pontificia Universidad Javeriana - Facultad de Ciencias Jurídicas
Maestría en Derecho Administrativo
Bogotá D.C.
2019

La responsabilidad demostrada frente al tratamiento de datos personales y su relevancia para la graduación de la sanción al interior de procedimientos administrativos sancionatorios

Diego Fernando Montezuma Chavez

Trabajo de grado para obtener el título de Magíster en Derecho Administrativo

Director: Manuel Eduardo Marín Santoyo

Pontificia Universidad Javeriana - Facultad de Ciencias Jurídicas
Maestría en Derecho Administrativo
Bogotá D.C.
2019

PONTIFICIA UNIVERSIDAD JAVERIANA - FACULTAD DE DERECHO
MAESTRÍA EN DERECHO ADMINISTRATIVO
PROYECTO DE INVESTIGACIÓN

LÍNEA DE INVESTIGACIÓN

Estado, Globalización, Derecho Administrativo, *Habeas Data*, *Big Data*, Tratamiento de Datos, Almacenamiento de datos, Transmisibilidad de Datos, Responsabilidad Civil.

TÍTULO DEL TRABAJO

La responsabilidad demostrada frente al tratamiento de datos personales y su relevancia para la graduación de la sanción al interior de procedimientos administrativos sancionatorios.

RESUMEN

El desarrollo social y empresarial ha tenido como consecuencia fenómenos tecnológicos que han impulsado al desarrollo del derecho en direcciones que no eran previsibles hace algunos años, de la misma manera en la cual las personas naturales han visto como dichos avances generan perfiles y acumulaciones de información que, en la mayoría de las ocasiones, puede considerarse lo suficiente importante para ser protegida por el derecho. Por las razones anteriormente expuestas, es que el presente documento tiene como fin la exposición del régimen de responsabilidad de las empresas por el incumplimiento de las disposiciones de protección de datos personales en Colombia.

PALABRAS CLAVE

Potestad Sancionadora de la Administración, Protección de Datos Personales, Principio de Responsabilidad Demostrada.

PONTIFICIA UNIVERSIDAD JAVERIANA – LAW FACULTY
MASTER IN ADMINISTRATIVE LAW
INVESTIGATION PROJECT

INVESTIGATION LINE

State, Globalization, Administrative Law, *Habeas Data*, Big Data, Data Processing, Data Storage, Data Transmissibility, Civil Liability.

TITLE

Demonstrate accountability in the processing of personal data and its relevance within the sanctions procedure to graduate the fin.

SUMMARY

Social and business development has resulted in technological phenomena that have led to the development of management law that were unforeseen some years ago, in the same way in which natural persons have seen such advances generate profiles and accumulations of information that, in most cases, it can be considered important enough to be protected by law. For the reasons stated above, the purpose of this document is to expose the corporate responsibility regime for non-compliance with the Personal Data protection provisions in Colombia.

KEY WORDS

Sanctioning Power of the Administration, Protection of Personal Data, Demonstrate accountability.

TABLA DE CONTENIDO

OBJETIVO GENERAL

El objetivo general del presente documento es identificar los elementos y criterios que ha tenido en cuenta la Superintendencia de Industria y Comercio -SIC- para aplicar el principio de responsabilidad demostrada como un factor de fijación de la sanción en las actuaciones administrativas sancionatorias adelantadas contra empresas responsables y encargadas del tratamiento de datos personales que han incumplido sus deberes establecidos en el artículo 17 de la Ley 1581 de 2012, Régimen de Protección de Datos Personales en Colombia, y demás normas concordantes.

OBJETIVOS ESPECÍFICOS

- Identificar en qué casos la Superintendencia de Industria y Comercio empleó criterios divergentes al momento de aplicar el principio de Responsabilidad Demostrada e imponer la sanción administrativa.
- Encontrar aquellos criterios que han sido reiterados en las decisiones en las que la Superintendencia de Industria y Comercio ha aplicado el principio de Responsabilidad Demostrada.
- Realizar un planteamiento crítico sobre la eficiencia del Régimen de Protección de Datos Personales en Colombia.

1. INTRODUCCIÓN

La importancia del tratamiento de los datos personales tiene especial relevancia en el mundo moderno toda vez que las grandes empresas y entidades de derecho público gracias a sus avances tecnológicos acumulan datos sensibles de las personas, por lo que ha surgido la necesidad de regular el tratamiento de los mismos, en especial teniendo en cuenta que los titulares de dichos datos pierden el dominio de estos, lo anterior, genera la necesidad de que se cimienten las bases de una ley de protección de estos. Sin perjuicio de lo mencionado, pareciera que la importancia en la Protección de Datos Personales continúa siendo un

concepto abstracto, y es por ello que tal vez la mejor manera de entenderlo sea mediante la ilustración de casos reales.

En cada oportunidad que se adquiere un servicio, se compra un producto en línea, se registra un correo electrónico a un *newsfeed*[1], cada vez que se realiza una visita médica, se pagan impuestos, se requiere de un bien o servicio, se están proporcionando datos personales a entidades de manera directa o indirecta. Incluso esta acumulación de datos es un fenómeno que ocurre en entidades con las cuales la persona aportante de los datos puede no tener contacto en ningún momento. Ante este escenario de recolección, administración, uso y explotación de datos personales, la única manera en la que puede el particular defenderse es mediante la expedición de normas estrictas para las prácticas anteriormente descritas, las cuales contengan preceptos normativos claros y sanciones administrativas eficientes y relevantes.[2]

Mediante la expedición de la Ley 1581 de 2012[3] y su Decreto Reglamentario 1377 de 2013[4], el Estado Colombiano actualizó sus políticas y compromisos en asuntos relacionados con la protección de datos personales, estipulando no solo aquellos presupuestos en los cuales se produce la vulneración de los intereses y los bienes jurídicos protegidos que se acoplan a la definición de datos personales, sino que adicionalmente reglamenta cuáles serán los eventos en los que se violen dichas disposiciones y cuál será el régimen correspondiente para su implementación.

[1] Página web o sección de la misma que se actualiza con frecuencia con el fin de mostrar las noticias actuales o información.

[2] A guide for policy engagement on Data Protection. The Keys to Data Protection. Privay International, Londres, Reino Unido, Agosto 2018. Documento consultado en https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf en agosto de 2019.

[3] Ley No. 1581. Diario Oficial No. 48587 de 18 de octubre de 2012.

[4] Decreto No. 1377. Diario oficial No. 48834 de junio 27 de 2013.

Así pues, con el fin de analizar la eficiencia y eficacia de las sanciones impuestas por la administración pública a través de la Superintendencia de Industria y Comercio por la violación de las disposiciones contenidas en la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013 a la luz del régimen de responsabilidad demostrada, se desarrolla el presente documento investigativo, en el cual se encontrará no solo una exposición de las disposiciones normativas nacionales, sino un cuadro de derecho comparado internacional respecto del tratamiento de datos personales y una mirada crítica y constructiva de la posición de la administración pública al momento de la imposición de sanciones.

2. LA POTESTAD SANCIONATORIA DE LA ADMINISTRACIÓN

Previo el abordaje puntual de las temáticas que desean desarrollarse en el presente documento, es menester generar un marco de contextualización en el que se exponga de donde proviene la facultad sancionatoria de la Superintendencia de Industria y Comercio por violación del *Habeas Data*.

Así pues, en primer lugar debe entenderse qué es la potestad sancionatoria de la Administración. En sentencia C-412 de 2015 la Honorable Corte Constitucional expresó que *"(l)a potestad sancionadora de la administración es una manifestación del ius puniendi estatal que consiste en la aplicación de medidas represivas por parte de las autoridades administrativas frente a los particulares (administrados) y a los servidores públicos cuando éstos incurren en actuaciones que afectan y/o amenazan el ordenamiento jurídico."*[5] O lo que es lo mismo, en otras palabras, la Potestad Sancionatoria del Estado es "*la reacción jurídica de la institucionalidad ante la vulneración de un precepto normativo establecido en interés general y cuya inobservancia debe ser reprimida."*[6] Lo anterior implica, como se observa, la imposición de limitaciones y deberes que deben de ser cumplidos por los administrados y que cuando se incumplen frustran expectativas de

[5] Sentencia C-412 de 2015, Corte Constitucional de Colombia, Magistrado Ponente Alberto Rojas Ríos.

[6] Resolución número 58194 del 31 de agosto de 2016, Superintendencia de Industria y Comercio.

derechos, situaciones que deben de corregirse y que llevan a la consignación de sanciones que implican la represión de la conducta del administrado que incumple.[7]

En consideración a lo anterior vale la pena mencionar que así como la demás actuaciones de la Administración, la aplicación de su potestad sancionatoria estará sujeta a unos principios:

i. El principio de legalidad, lo cual implica la existencia de una ley regulatoria.

ii. El principio de tipicidad que, el cual implica la necesidad de que se realice una descripción de la conducta que da lugar al nacimiento de la Potestad Sancionadora de la Administración, así como la determinación expresa de la sanción.

iii. El debido proceso, principio que implica la existencia de un procedimiento claro, y así mismo asegurar el derecho de defensa del sancionado.

iv. El principio de proporcionalidad, el cual implica una proporción entre a sanción y la falta cometida.

v. La independencia de la sanción penal[8].

Principios que no podrán ser obviados o ignorados al momento de materializarlos en la aplicación de sanciones por violación a las disposiciones de protección del *Habeas Data*, como se observará mas adelante en el desarrollo del presente documento.

Finalmente, desde el ámbito puramente administrativo, debemos referirnos al artículo 47 de la Ley 1437 de 2011[9] (Código de Procedimiento Administrativo y de lo Contencioso Administrativo), el cual expresa que la administración, una vez finalizada la etapa de averiguaciones preliminares:

> *"(F)ormulará cargos mediante acto administrativo en el que señalará, con precisión y claridad, los hechos que lo originan, las personas naturales o*

[7] Si se desea profundizar en la naturaleza jurídica de la Potestad Sancionatoria de la Administración se puede referir a la sentencia C – 875 de 2011, M. P. Jorge Ignacio Pretelt Chaljub.

[8] Para mayor información sobre el desarrollo de los principios de la Potestad Sancionadora de la Administración revisar las sentencias C-616 de 2002, C-595 de 2010, C-089 de 2011 y C-748 de 2011.

[9] Ley No. 1437. Diario Oficial No. 47956 de 18 de enero de 2011.

jurídicas objeto de la investigación, las disposiciones presuntamente vulneradas y las sanciones o medidas que serian procedentes. Este acto administrativo deberá ser notificado personalmente a los investigados. Contra esta decisión no procede recurso.

Los investigados podrán, dentro de los quince (15) días siguientes a la notificación de la formulación de cargos, presentar los descargos y solicitar o aportar las pruebas que pretendan hacer valer. Serán rechazadas de manera motivada, las inconducentes, las impertinentes y las superfluas y no se atenderán las practicadas ilegalmente".

De la lectura de la norma, se observa que el artículo 47 de la Ley 1437 de 2011 acata de manera cabal con los principios decantados por la jurisprudencia para la aplicación de la Potestad Sancionatoria del Estado.

Desde un ámbito puramente doctrinario debemos entender la potestad sancionadora de la Administración como "*El poder jurídico para imponer decisiones a otros para el cumplimiento de un fin. La potestad entraña, así, un poder otorgado por el ordenamiento jurídico de alcance limitado o medido para una finalidad predeterminada por la propia norma que la atribuye, y susceptible de control por los tribunales. La potestad no supone, en ningún caso, un poder de acción libre, según la voluntad de quien lo ejerce, sino un poder limitado y controlable. Dentro de las potestades, las de la Administración Pública son potestades–función, que se caracterizan por ejercerse en interés de `otro´, esto es, no de quien la ejerce, sino del interés público o general".*[10]

Como lo expresa Juan Manuel Laverde Álvarez en su libro "*La Potestad Sancionadora de la Administración",* esta misma es una fuerza del Derecho Público la cual se encuentra integrada por un haz de facultades entre las que cabe destacar la de establecimiento normativo, la de imposición y la de ejecución.[11] De lo anterior se concluye que la imposición

[10] Luis Cosculluela Montaner, Manual de Derecho Administrativo, Tomo I, 17ª Edición, Madrid, Thomson Civitas, 2006, página 336.

de la sanción responderá a un principio de legalidad, concretándose por tanto mediante la expedición de un acto administrativo por parte de la Administración Pública.
Con miras a contextualizar la Potestad Sancionadora de la Administración cabe mencionar cuáles son sus características de acuerdo a aquellas identificadas por Laverde Álvarez[12]:

- La Potestad Sancionadora de la Administración busca la materialización de los principios constitucionales.
- Esta es la respuesta del Estado a la inobservancia de las obligaciones impuestas a los administrados para el debido funcionamiento del Estado.
- La Potestad Sancionadora de la Administración se ejerce desde la vulneración de las reglas jurídicas preestablecidas.
- Respecto de las sanciones impuestas se encuentran prohibidas las sanciones privativas de la libertad.
- Como cualquier otro Acto Administrativo, aquel que imponga la sanción estará sujeto a control judicial ante la Jurisdicción de lo Contencioso Administrativo.

2.1. FACULTAD SANCIONADORA EN CABEZA DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Con el fin de poder explicar a cabalidad la facultad sancionadora por la violación del Régimen de Protección de Datos Personales en Colombia debe primero contextualizarse en cabeza de quien se encuentra dicha potestad, siendo este organismo la Superintendencia de Industria y Comercio.

Tras la primera mitad del siglo XX en Colombia se hace necesaria la presencia de un organismo con la facultad de recolectar las funciones que tradicionalmente se encontraban diseminadas en diferentes ministerios e instituciones, y es así como nace, mediante la Ley 19

[11] Para mayor información consultar a Juan Manuel Laverde Álvarez, Manual de Procedimiento Administrativo Sancionatorio, 2ª Edición, LEGIS Editores S.A., 2018.
[12] Juan Manuel Laverde Álvarez, Manual de Procedimiento Administrativo Sancionatorio, 2ª Edición, LEGIS Editores S.A., 2018, página 17 y siguientes.

de 1958[13] y el Decreto 1653 de 1960[14], la Superintendencia de Regulación Económica, organismo ejecutivo cuya principal función era estudiar y aprobar, mediante su criterio económico, los varios reglamentos y tarifas de cada uno de los servicios públicos.

El 29 de junio de 1999, mediante la expedición del Decreto 1130 [15] se le da a la Superintendencia de Industria y Comercio la facultad de inspeccionar y vigilar todo lo que se vea relacionado con el régimen de libre competencia y competencia desleal en los servicios no domiciliarios en comunicaciones, al tiempo que se le otorgó la protección de los derechos de los usuarios de servicios no domiciliarios de telecomunicaciones.

Por lo anterior es que se debe entender que es la Superintendencia de Industria y Comercio la entidad llamada, naturalmente, a conocer los supuestos fácticos de infracciones al régimen de protección de datos personales, y por tanto, haciendo uso de su potestad sancionadora, condenar a los infractores en los términos que más adelante se tratarán.

2.1.1. FACULTAD SANCIONATORIA POR VIOLACIÓN DEL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

De acuerdo a lo anteriormente expuesto, y en concordancia con las disposiciones legales que regulan la materia, se observa que la Superintendencia de Industria y Comercio tiene las facultades legales y sancionadoras necesarias para imponer penas a aquellas personas que, por su actuar, violen las disposiciones del Régimen de Protección de Datos Personales en Colombia.

Así pues, la facultad se deriva de la norma jurídica, en este caso los artículos 22, 23 y 24 de la Ley 1581 de 2012, en concordancia con el artículo 18, *ibidem*, el cual brinda a la Superintendencia de Industria y Comercio la autoridad para ejercer la vigilancia y control

[13] Ley No. 1581. Diario Oficial No. 29835 de 9 de diciembre de 1958.
[14] Decreto 1653. Diario Oficial No. 30301 de 10 de agosto de 1960.
[15] Decreto No. 1130. Diario Oficial No. 43625 de 29 de junio de 1999.

que garantice el debido tratamiento de datos personales y que se respeten los principios, derechos, garantías y procedimientos previstos en la ley.[16]

El artículo 22, *ibidem*, regula el trámite para la imposición de sanciones, expresando que una vez la Superintendencia de Industria y Comercio verifique la infracción de las disposiciones, por parte del Responsable de Tratamiento o Encargado de Tratamiento, adoptará las medidas necesarias o impondrá las sanciones correspondientes.[17] Vale la pena llamar la atención sobre la aparente disyuntiva de la norma, toda vez que parece implicar que la Superintendencia de Industria y Comercio podrá (i) tomar las medidas necesarias para asegurar la cesación en la infracción, o (ii) imponer las sanciones correspondientes, escenario el cual no tendría sentido, pues la imposición de sanciones sin la implementación de acciones reales que obliguen la cesación de la infracción por el infractor no garantiza en si misma dicha cesación.

16 En virtud del artículo 21 de la Ley 1581 de 2012, la Superintendencia de Industria y Comercio tendrá las siguientes funciones en lo referente a la protección de datos personales en Colombia:
"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."

17 Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, Artículo 22, Trámite.

El artículo 23, *ibidem*, lista las sanciones que la Superintendencia de Industria y Comercio podrá imponer a quienes hayan infringido las disposiciones del Régimen de Protección de Datos Personales, las cuales tomarán las siguientes formas:

- Multas de hasta 2.000 salarios mínimos legales mensuales vigentes que podrán ser sucesivas en tanto subsista la sanción.
- 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
- 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;
- Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

Finalmente, el artículo 24 de la ley 1581 de 2012 establece los criterios por los cuales se deben de graduar las sanciones anteriormente expuestas, entre los que se encuentran: *"(i) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley; (ii) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción; (iii) La reincidencia en la comisión de la infracción; (iv) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio; (v) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio; (vi) 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".*

3. IMPORTANCIA DEL SISTEMA GENERAL DE PROTECCIÓN DE DATOS PERSONALES, CONTEXTUALIZACION Y ANÁLISIS

Previo el estudio del Sistema de Protección de Datos Personales en Colombia es necesario entender conceptualmente qué son datos personales. Así pues, la ley 1581 de 2012 establece

que Dato Personal es *"Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables".*[18]

Sin perjuicio de la definición legal, parece que la misma no agota el concepto total y no logra expresar la importancia de la definición de los mismos. En este sentido nos remitimos a los pronunciamientos de la Corte Constitucional, la cual ha profundizado el entendimiento del concepto de datos personales y *Habeas Data*. En efecto, esa Corporación expresó:

> *"En la jurisprudencia constitucional, el derecho al habeas data fue primero interpretado como una garantía del derecho a la intimidad, de allí que se hablara de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir. También, desde los primeros años de la nueva Carta, surgió al interior de la Corte una segunda línea interpretativa que consideraba el habeas data una manifestación del libre desarrollo de la personalidad (…) surge una tercera línea interpretativa que es la que ha prevalecido desde entonces y que apunta al habeas data como un derecho autónomo, en que el núcleo del derecho al habeas data está compuesto por la autodeterminación informática y la libertad –incluida la libertad económica. Este derecho como fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben pender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones."*[19]

Aun así, los conceptos legales no explican cabalmente la importancia de los datos personales, y por ello es menester referirnos a otros mas amplios como lo son la economía, la sociología

[18] Ley estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, artículo 3º, Definiciones.
[19] Sentencia C – 748 de 2011, Magistrado Ponente Jorge Ignacio Pretelt Chaljub.

y la tecnología, entre otros. De la conjunción de estos nace lo que hoy en día conocemos como *BIG DATA*, "*la cual se refiere al proceso de examinar enormes cantidades de datos de diversa variedad o naturaleza para extraer de ellos patrones, correlaciones o conclusiones que puedan ser útiles para realizar predicciones o adoptar decisiones*[20]. El asunto problemático entonces es, ¿de quién son estos datos? ¿Cómo se recolectan? ¿Qué uso se les puede dar? Estas son algunas de las preguntas que desean contestarse mediante el presente documento. Sin perjuicio de lo anterior, debe entenderse igualmente la importancia de formularse estas preguntas, pues sin ellas no existiría un régimen de responsabilidad aplicable a los incumplimientos y violaciones de las disposiciones nacionales e internaciones sobre el uso de datos, lo cual nos llevaría a pensar que todo está permitido en la recolección, almacenamiento y uso de datos de naturaleza personal.

Al respecto, es menester traer a colación las apreciaciones que al respecto formula Nelson Remolina Angarita cuando escribe:

> "*Los beneficios y las consecuencias adversas del big data dependerán del uso ético y responsable que haga quien posee enormes cantidades de datos sobre diversos aspectos de millones de personas alrededor del mundo. Con la tecnología se puede hacer casi todo. La pregunta que surge es la siguiente: todo lo tecnológicamente posible, ¿es social y humanamente deseable?"*[21]

Para responder a esta pregunta pueden citarse situaciones tan concretas como fueron la posición de IBM frente al holocausto judío en el marco de la Segunda Guerra Mundial[22] o el

[20] Nelson Remolina Angarita, Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012, Primera Edición, LEGIS Editores S.A., 2013, página 3 y siguientes. "*La expresión big data no significa solamente "grandes datos" sino, ante todo, las grandes cosas que se pueden hacer con incalculables cantidades de información. Se basa en el uso de ingentes volúmenes de datos que son analizados y relacionados desde diferentes variables para sacar conclusiones, innovar, predecir, tomar decisiones, adoptar estrategias, entre otras. Es una especie de "minería de datos" avanzada y a gran escala que se gestó desde el Siglo XX y se realiza sobre muchísimos datos de diversa naturaleza y origen.*"

[21] Nelson Remolina Angarita, Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012, Primera Edición, LEGIS Editores S.A., 2013, página 5.

[22] Cuando el Tercer Reich se embarcó en su plan de conquista y genocidio de los judíos, IBM y sus subsidiarias ayudaron a crear tecnologías que posibilitaron programas de identificación y clasificación desconocidos hasta

papel que jugó Facebook en el escándalo de recolección y uso de datos personales de millones de personas por parte de Cambridge Analytica con fines de publicidad política.[23]

Por todo lo anteriormente expuesto es que debe de entenderse el concepto de los datos personales como una posibilidad, al tiempo que como una responsabilidad social y un foco de oportunidades y consecuencias mas allá de lo estrictamente jurídico, y es allí, en su núcleo como Derecho Fundamental y en su importancia en la vida de las personas, en donde encuentra raíz y razón de ser el Sistema de Protección de Datos Personales al cual se refiere en páginas siguientes.

3.1. ÁMBITO INTERNACIONAL

En primer lugar debe de mencionarse que al ser el fenómeno de tratamiento de datos personales relativamente nuevo (especialmente cuando se compara con instituciones jurídicas como la propiedad privada o la compraventa), no hay unanimidad en la forma en la que deben los Estados regular y legislar sobre el proceso, como la recolección, la guarda y el uso de dichos datos. Por lo anterior es que a nivel internacional se pueden identificar corrientes que han regulado y dado unas pautas específicas para la protección de datos personales, entre las que podemos identificar:

3.1.1. EL SISTEMA DE PROTECCIÓN DE DATOS PERSONALES EN LA UNIÓN EUROPEA

La regulación europea en tema de protección de datos personales estriba, básicamente, en la concepción del sistema de protección como un conjunto de normas de carácter general que

ese momento. Sólo después de haber identificado a los judíos -una tarea monumental y compleja que Hitler quería terminada de inmediato-, se podía lograr una eficiente confiscación de bienes, reclusión en ghettos, deportación, explotación laboral y, en última instancia, aniquilación. Para mayor información consultar IBM y el Holocausto: La alianza estratégica entre la Alemania Nazi y la corporación más poderosa de América de Edwin Black.

[23] https://www.bbc.com/mundo/noticias-49093124 consultado en Septiembre de 2019.

encuentran sus particularidades en cada uno de los países que componen la Unión Europea, a la vez que contempla la existencia de una autoridad de control encargada de hacer cumplir dichas disposiciones[24]. Aunado a lo anterior, vale la pena mencionar que tal vez una de las principales particularidades y avances del sistema europeo de protección de datos personales es el hecho de que los mismos son concebidos con la categoría de Derechos Fundamentales. Así pues, La *European Data Protection Supervisor* expone en su página web que para la Unión Europea la dignidad humana es un derecho fundamental absoluto, y en tal sentido la noción de la dignidad implica el derecho a tener una vida privada, a la autonomía de la persona y a que esta pueda controlar su propia información, pues la privacidad no es únicamente un derecho sino un valor social. [25]

Lo anterior permite entonces comprender el altísimo nivel de importancia que otorgan los organismos del sistema europeo de protección de derechos a los datos personales y consecuentemente a su protección, debido manejo y sanciones consecuentes con el desacato de las directrices impartidas.

Con el fin de ilustrar el alcance de la concepción del sistema europeo de la protección de datos personales como un derecho fundamental es menester mencionar el caso T-161/04: Judgment of the General Court del 7 de Julio 2011 - Valero Jordana v Commission, caso en el cual se expresó:

> "(*P)rocede recordar que, conforme a su artículo 1, apartado 1, el Reglamento nº 45/2001 tiene por objeto garantizar «la protección de los derechos y las libertades fundamentales de las personas físicas, y en particular su derecho a la intimidad, en lo que respecta al tratamiento de los datos personales» y que las*

[24] Dicha entidad tiene el nombre de Comité Europeo de Protección de Datos (EDPB por sus siglas en ingles) y su finalidad es contribuir "a la aplicación coherente de las normas de protección de datos en toda la Unión Europea" y promover "la cooperación entre las autoridades de protección de datos de la UE." https://edpb.europa.eu/about-edpb/about-edpb_es consultado en octubre de 2019.

[25] "*In the EU, human dignity is recognized as an absolute fundamental right. In this notion of dignity, privacy or the right to a private life, to be autonomous, in control of information about yourself, to be let alone, plays a pivotal role. Privacy is not only an individual right but also a social value*." Consultado en https://edps.europa.eu/data-protection/data-protection_en en septiembre de 2019.

personas susceptibles de ser protegidas son aquellas cuyos datos personales son tratados por las instituciones u organismos comunitarios en cualquier contexto, por ejemplo, porque estas personas estén empleadas por dichas instituciones u organismos (…).”[26]

En igual sentido falla el Tribunal de justicia de la Unión Europea en la sentencia C28-08-P de 26 de junio de 2010, en la que expresa:

“Por último, el Tribunal consideró que la excepción prevista en el artículo 4, apartado 1, letra b), del Reglamento nº 1049/2001 debía interpretarse de manera restrictiva y sólo afectaba a los datos personales que pueden, de forma concreta y efectiva, suponer un perjuicio para la protección de la intimidad y la integridad de la persona. El examen de tal perjuicio debe efectuarse a la luz del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma el 4 de noviembre (en lo sucesivo, «CEDH») y de la jurisprudencia desarrollada en base a él.”[27]

3.1.2. EL SISTEMA DE PROTECCIÓN DE DATOS PERSONALES EN ESTADOS UNIDOS DE AMÉRICA

El sistema estadounidense de protección de datos se caracteriza a su vez por tener una mezcla de legislación, reglamentación y autorregulación[28], lo cual se puede evidenciar con claridad en la concepción de este país sobre tal escenario. Mientras que el sistema europeo lo considera un Derecho Humano Fundamental, el estadounidense lo considera un derecho del consumidor. Como lo expone Nelson Remolina Angarita:

---

[26] Caso T-161/04: Judgment of the General Court del 7 de Julio 2011 - Valero Jordana v Commission. Consultado en http://curia.europa.eu/juris/document/document.jsf;jsessionid=39DFF15AB6BA49BA49F4F9289FDB4FCE?text=&docid=114846&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=1944018 en noviembre de 2019.

[27] Caso C28-08-P del 26 de junio de 2010, consultado en http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d519e2ce8308964a23a91af1df8b7d4ed3.e34KaxiLc3eQc40LaxqMbN4Oa3aKe0?text=&docid=84752&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=228738 en Noviembre de 2019.

[28] Nelson Remolina Angarita, Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012, Primera Edición, LEGIS Editores S.A., 2013, página 19.

> "*El enfoque norteamericano sobre esta materia no considera la protección de datos como un derecho fundamental, sino como un derecho del consumidor. Está integrado por algunas disposiciones sectoriales y no estima necesaria la existencia de las autoridades de control especializadas en tratamiento de datos personales, sin perjuicio de que tenga otras formas de control. Esta visión prefiere la autorregulación y la promulgación de varias normas sectoriales, en lugar de disposiciones generales."*[29]

Respecto de la coexistencia de estos dos modelos de protección de datos personales en un mundo globalizado e integrado debe concluirse que la concepción norteamericana, la cual considera la protección de datos como un derecho del consumidor, y la concepción europea, que le considera un derecho fundamental, en la práctica ha implicado negociaciones y esfuerzos globales tendientes a esquemas de unificación, o al menos a encontrar puntos de convergencia. Como expone Nelson Remolina Angarita, "*La Comisión Europea, mediante Decisión 2000/520/CE del 26 de julio, decidió que los Principios de puerto seguro, aplicados de conformidad con la orientación que proporcionan las preguntas más frecuentes (FAQ), publicadas por el Departamento de Comercio de Estados Unidos, garantizan un nivel adecuado de protección de datos personales transferidos desde la Comunidad a entidades establecidas en Estados Unidos de América."*[30]

3.1.3. SISTEMAS DE AUTORREGULACIÓN

La mayoría de los sistemas de protección de datos personales a nivel mundial se encuentran acompañados por fenómenos de autorregulación, los cuales se pueden entender como las disposiciones de un grupo de personas o entidades con un aspecto en común y que tiene como

[29] Nelson Remolina Angarita, Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012, Primera Edición, LEGIS Editores S.A., 2013, página 19 – 20.

[30] Nelson Remolina Angarita, Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012, Primera Edición, LEGIS Editores S.A., 2013, página 19

fin el establecimiento de políticas y pautas de conducta para el tratamiento de un asunto en específico, como lo es el de datos personales.[31]

Aun cuando las disposiciones autorregulatorias de un Sistema de Protección de Datos Personales son deseables, es claro que un sistema en el cual se es juez, verdugo y parte no puede ser el mas eficiente, por lo cual deben de tenerse en cuenta los siguientes aspectos:

i. La autorregulación no sustituye el papel de regulación del Estado y su labor;
ii. La autorregulación puede tener un efecto de fortalecimiento de la protección de las personas siempre que cuente con las herramientas necesarias para hacer cumplir sus disposiciones;
iii. Es necesario contar con mecanismos que permitan la verificación de cumplimiento de las disposiciones del autorregulador[32].

Para finalizar, y previo a entrar en un análisis integrado del sistema latinoamericano, y puntualmente colombiano, de protección de datos personales, es menester hacer una reflexión sobre los esfuerzos que se hacen desde diferentes escenarios por una protección de datos personales de carácter global. Como expresan Ornelas Núñez e Higuera Pérez:

> *"Nuestro mundo se encuentra girando en una imparable espiral de innovación. La tecnología brinda infinitas posibilidades de procesar y utilizar información. Esto facilita a los individuos el desarrollo de sus actividades pero también aumenta los riesgos de ser afectado por el uso ilegítimo de esta. La preocupación derivada de estos riesgos ha sido atendida por las distintas regiones del mundo a través de regulaciones en materia de protección de datos. No obstante, estas visiones —y regulaciones— tienen claros limitantes territoriales que no permiten una protección global a un fenómeno global. La autorregulación aparece como*

[31] Otros ejemplos del fenómeno de la autorregulación en Colombia son: el Autorregulador del Mercado de Valores y el Autorregulador Nacional de Avaluadores.

[32] Nelson Remolina Angarita, Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012, Primera Edición, Legis, 2013, página 25.

una herramienta capaz de ampliar la protección de los individuos más allá de las fronteras (…)"[33]

De acuerdo a lo que se ha expresado anteriormente en el presente documento es claro que la transmisión, almacenamiento y tratamiento de datos personales son un fenómeno intrínseco a la globalización, la prestación de servicios y el comercio internacional, por lo cual es importante que el derecho, respondiendo a las necesidades de unas realidades innegables, de lugar a nuevas figuras de carácter nacional y supranacional, como es la autorregulación vinculante, figura la cual tiene todos los beneficios de una norma legal con la particularidad de imponer disposiciones hechas a la medida por quien las acaten.

3.1.4. EL SISTEMA DE PROTECCIÓN DE DATOS EN AMERICA LATINA

Sostiene Remolina Angarita[34] que los sistemas latinoamericanos, como el colombiano, se han visto altamente influenciados por la visión garantista del Sistema Europeo. Lo anterior se puede evidenciar, principalmente, en los pronunciamientos emanados por la Corte Constitucional respecto de los datos personales que, dan la categoría de Derecho Fundamental al *Habeas Data*, como se explicara y ahondará a continuación.[35]

[33] Para mayor información consultar La autorregulación en materia de protección de datos personales: la vía hacia una protección global, Lina Gabriela Ornelas Núñez y Melissa Higuera Pérez, Revista de Derecho, Comunicaciones y Nuevas Tecnologías No. 9, Universidad de Los Andes, Facultad de Derecho, Junio 2013.

[34] Nelson Remolina Angarita, Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012, Primera Edición, Legis, 2013, página 26.

[35] Los pronunciamientos más relevantes de la Honorable Corte Constitucional en materia de protección de datos personales son la sentencia C – 748 de 2011 y la sentencia C-1011 de 2008, sentencias en las cuales la corte expresó que "Dentro de las prerrogativas o contenidos mínimos que se desprenden del derecho al *habeas data* encontramos por lo menos las siguientes: (i) el derecho de las personas a conocer –acceso- la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a incluir nuevos datos con el fin de se provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa. (Sentencia C-748 de 2011, Magistrado Ponente Jorge Ignacio Pretelt Chaljub).

3.1.5. OBSERVACIONES FINALES DE LOS SISTEMAS DE PROTECCIÓN DE DATOS A NIVEL INTERNACIONAL

Es claro por más que las disposiciones legales nacionales, internacionales y supranacionales actuales no son una respuesta suficiente a los rápidamente cambiantes fenómenos tecnológicos que permiten una masiva recolección y tratamiento de datos personales, por lo cual, como lo expresa Recio Gayo, "*(l)os datos personales masivos requerirán una aproximación diferente a la actual, lo que implica que deban seguirse altos estándares internacionales en materia de protección de datos personales, privacidad y ciberseguridad, si se quiere alcanzar una protección efectiva de la persona."* Continúa Recio Gayo expresando que sin perjuicio de las actuaciones internacionales en protección de datos personales, *"hay que prestar atención específica- mente a que el marco sobre la protección de datos personales y la privacidad sea el adecuado para proteger a la persona en sus derechos fundamentales; garantizar el libre flujo internacional de los datos personales; facilitar la innovación; evitar medidas proteccionistas arbitrarias o injustificables y, al mismo tiempo, impulsar la competitividad."*[36]

3.2. EL SISTEMA DE PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

Con miras a realizar un análisis conducente y eficiente del Sistema de Protección de Datos Personales en Colombia se procederá en primer lugar al análisis de los derechos y disposiciones constitucionales relacionadas con los datos personales, para, de esta manera, continuar con el análisis de los preceptos legales que regulen la materia.

3.2.1. ÁMBITO CONSTITUCIONAL

Desde una perspectiva constitucional, el Régimen General de Protección de Datos Personales en Colombia encuentra su asidero en los artículos 15, 16 y 20 de la Carta Política, los cuales establecen que:

[36] Miguel Recio Gayo, Big Data: Hacia la protección de Datos Personales basada en una transparencia y responsabilidad aumentadas, Revista de Derecho, Comunicaciones y Nuevas Tecnologías, Universidad de los Andes, Facultad de Derecho, No. 17, enero – junio 2017, página 8.

> *"**ARTÍCULO 15.** Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*
>
> *En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución."*
>
> ***ARTICULO 16.** Todas las personas tienen derecho al libre desarrollo de su personalidad sin más limitaciones que las que imponen los derechos de los demás y el orden jurídico.*
>
> ***ARTICULO 20.** Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.*
> *Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura."*

Las disposiciones anteriormente mencionadas han dado paso al reconocimiento del derecho fundamental autónomo que ha sido catalogado como el *Habeas Data*, o también llamada como la autodeterminación informativa o informática. A pesar de lo anterior, en sentencia C – 748 de 2011, la Honorable Corte Constitucional concluyó que la Ley 1581 de 2012 (*Por la cual se dictan disposiciones generales para la protección de datos personales*), no abarca en su totalidad el desarrollo total de los artículos constitucionales mencionados. Tanto es así que expresa:

> *"Sobre el segundo y tercer objetivos, la Corte encuentra que son demasiado amplios si se comparan, por una parte, con el título del proyecto y el contenido del articulado y, por otra, con las garantías comprendidas en los artículos 15 y 20 superiores.*

> *En efecto, el artículo 15 de la Carta reconoce tres derechos: (i) el derecho a la intimidad, (ii) el derecho al buen nombre y (iii) el derecho al habeas data. La Sala observa que si bien el derecho al habeas data está estrechamente ligado con los derechos a la intimidad y al buen nombre, todos los anteriores son derechos con contenidos autónomos y diferentes. En este caso, la Sala encuentra que el proyecto solamente pretende desarrollar el habeas data y no los otros derechos, por lo que si bien la disposición no desconoce la Carta por ser amplia en este respecto, debe entenderse que solamente desarrolla indirectamente los derechos a la intimidad y al buen nombre, es decir, no puede considerarse una regulación comprensiva y sistemática de tales derechos."*[37]

Sin perjuicio de lo anterior, mediante sentencia C – 1011 de 2008, M.P. Jaime Córdoba Triviño, la Honorable Corte Constitucional expresó:

> *"El derecho al hábeas data es definido por la jurisprudencia constitucional como aquel que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, de conformidad con los principios que regulan el proceso de administración de datos personales. Este derecho tiene naturaleza autónoma y notas características que lo diferencian de otras garantías con las que, empero, está en permanente relación, como los derechos a la intimidad y a la información."*[38]

Por lo anteriormente expuesto, no sólo en este acápite sino en anteriores al haber hecho referencia a los sistemas internacionales que han afectado el desarrollo del sistema colombiano de protección de datos personales, al hacer referencia a las falencias de un

[37] Sentencia C – 748 de 2011, numeral 2.3.3.3., Honorable Corte Constitucional de Colombia, Magistrado Ponente Jorge Ignacio Pretelt Chaljub.

[38] Sentencia C – 1011 de 2008, Honorable Corte Constitucional de Colombia, Magistrado Ponente Jaime Córdoba Triviño.

método de autorregulación y al tener claro el rango constitucional del derecho al *Habeas Data*, se puede proceder ahora a explicar, de una manera más completa y extensa el Régimen General de Protección de Datos Personales en Colombia.

3.2.2. RÉGIMEN GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

3.2.2.1. ANTECEDENTES

Con el fin de realizar el debido estudio del Régimen General de Protección de Datos Personales en Colombia es menester proceder, inicialmente, con el análisis de los antecedentes legislativos de la Ley 1581 de 2012. En este sentido, y con el fin de realizar una exposición clara de tales referencias, se examinaran las gacetas del Congreso de la República relevantes para la aprobación de la ley anteriormente mencionada.

- **Proyecto de Ley 046 de 2010**

En primer lugar debe traerse a colación el proyecto de ley 046 de 2010, el cual fue presentado el día 03 de octubre de ese año por los señores Ministros de Interior y de Justicia, Fabio Valencia Cossio; de Comercio, Industria y Turismo, Luis Guillermo Plata Páez y de Tecnologías de la Información y las Comunicaciones, Daniel Enrique Medina Velandia, ante la Secretaría General de la Cámara de Representantes.

Dentro de la exposición de motivos se expresa que la necesidad de una norma que regule el derecho al *Habeas Data* nace de la realidad que es en el mundo actual la automatización en los procesos de recolección y tratamiento de datos personales, lo cual plantea no pocas incertidumbres a quienes facilitan dichos datos, pues en la mayoría de las ocasiones se desconoce la finalidad del tratamiento, facilitando así transacciones poco éticas o que atenten contra los mejores intereses de los particulares que proporcionan sus datos personales.

> *"Esto significa que su recolección, almacenamiento, registro, uso o divulgación* (de los datos) *se garantice que desde el otorgamiento del consentimiento por parte del Titular para que sean utilizados con los fines que se le indiquen, hasta el momento en que tal uso se efectué legítimamente por parte de un tercero, se hayan utilizado altos estándares de calidad en el manejo de la información al tiempo que se le otorguen claras herramientas al Titular para exigir medidas concretas de protección frente a cualquier vulneración de que pudiera ser víctima."*[39]

Adicionalmente y como refuerzo de los argumentos de los señores ministros, se cita la sentencia C – 1011 de 2008, la cual expresa:

> *"El derecho al hábeas data es definido por la jurisprudencia constitucional como aquel que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, de conformidad con los principios que regulan el proceso de administración de datos personales. Este derecho tiene naturaleza autónoma y notas características que lo diferencian de otras garantías con las que, empero, está en permanente relación, como los derechos a la intimidad y a la información."*[40]

El proyecto de ley anteriormente mencionado, con su correspondiente exposición de motivos, fue publicado el 4 de agosto en la Gaceta del Congreso No. 488 de 2010, dando cumplimiento al requisito constitucional consistente en la publicación oficial del proyecto antes de darle curso en la Comisión respectiva.

A continuación se procederá con el análisis de las diferentes gacetas del Congreso en las cuales se hicieron los correspondientes debates para la expedición de la Ley 1581 de 2012:

---

[39] Proyecto de ley 046 de 2010, Exposición de Motivos, Antecedentes.

[40] Corte Constitucional, Sentencia C – 1011 de 2008, Magistrado Ponente Jaime Córdoba Triviño.

- **Gaceta del Congreso 625 de 09 de septiembre de 2010**

Mediante la presente Gaceta del congreso se expresa que para todos los efectos del proyecto de ley discutido, el concepto de Dato Personal reúne las siguientes características: i) estar referido a aspectos exclusivos y propios de una persona natural; ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión en conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera licita o ilícita; y iv) su tratamiento está sometido a reglas especiales en lo relativo a su captación, administración y divulgación.[41]

Adicionalmente se llama la atención sobre la falta de una ley de protección de datos personales, toda vez que al momento de la plenaria expuesta se presentaban en Colombia normas legales de carácter sectorial que no daban una protección holística y eficiente a los titulares de datos personales. Como consecuencia de lo anterior se hizo visible la necesidad de la población de contar con herramientas legales como titulares de datos para que mediante estas tuvieran la facultad de salvaguardar sus derechos ante los Responsables y Encargados de Tratamiento.

Expresa la Gaceta del Congreso 625 del 09 de septiembre de 2010 que:

> *"En el Siglo XXI el dato personal se constituye como la "materia prima" para el desarrollo del sector de servicios y en especial para el de los procesos de negocio tercerizados a distancia. Esta situación evidencia, a diferencia del caso de los bienes donde existe un control manifiesto por su naturaleza, la necesidad de desarrollar mecanismos legales internacionales que permitan que los datos estén protegidos, brindando así una garantía al titular de la información."*[42]

[41] Gaceta del Congreso 625 del 09 de septiembre de 2010, página 2.
[42] Gaceta del Congreso 625 del 09 de septiembre de 2010, página 4.

Finalmente, entre las modificaciones realizadas por parte del Congreso y expuestas en la Gaceta 625, cabe mencionar el hecho que desde los primeros artículos se haga presente que el ente de control, quien impone las sanciones, es la Superintendencia de Industria y Comercio, toda vez que en el proyecto de ley inicial no dejaba este hecho claro hasta su artículo 19.[43]

- **Gaceta del Congreso 706 de 28 de Septiembre de 2010**

Mediante la Gaceta del Congreso 706 de 2010 se hacen presentes en las deliberaciones los muy significativos aspectos económicos que se derivan de la protección de datos y en este sentido se expresa que aun cuando existen condiciones económicas y políticas atractivas para que Colombia desarrolle un sector de tercerización de servicios, es importante competir no únicamente en términos de costos, sino en un ambiente legal atractivo para los inversionistas extranjeros.

> *"Para lograr esto, en primera instancia es necesario desarrollar un marco normativo que incorpore los más altos estándares internacionales en protección de datos personales y permita posicionar el país como un puerto seguro para la tercerización de servicios.*
> *(…)*
> *Las reformas sectoriales, sumadas a la inversión en el sector, permitieron que el país mejorara en los índices de competitividad, es así como en el reporte del Foro Económico Mundial sobre el progreso de las TIC Colombia escaló nueve posiciones entre 2008 y 2010 y seis posiciones en el índice e-readiness ranking de la revista The Economist en el período 2008-2009.*
>
> *Está claro entonces que un adecuado marco normativo que incorpore estándares internacionales y que equilibre la libertad de empresa, vigilancia y control por*

[43] Gaceta del Congreso 625 del 09 de septiembre de 2010, página 14.

parte del Estado y adecuados estímulos a la inversión es necesario para atraer inversiones a un sector.” [44]

Por lo anterior se hace clara entonces la importancia de la adecuación de una legislación nacional a los mas altos estándares internacionales en materia de protección de datos personales, permitiendo así que Colombia, en dicha oportunidad, se adecuara a las directrices internacionales en materia de *Habeas Data*, acercándose por este medio a la implementación del Principio de Responsabilidad Demostrada, concepto que se explicara oportunamente en el desarrollo del presente documento.

- **Gaceta del Congreso 958 del 24 de Noviembre de 2010**

La presente Gaceta del Congreso pone de presente la importancia del proyecto de ley y su aprobación, pues mediante estos se “*nos abren las puertas para empezar nosotros como país, posicionándonos dentro de la espera Suramericana y mundial, como proveedor de servicios a terceros: en esta medida nosotros evidenciamos que la no inclusión, o la no tenencia de una ley de este tipo por nuestra parte, no ha hecho posible que nosotros tengamos la posibilidad de ser objeto de transferencia de información, de países pertenecientes por ejemplo a la Unión Europea y en esa medida eso nos limita la posibilidad, de que sean las empresas colombianas o empresas colombianas contratadas, con fines de prestación de servicios en el exterior.”*[45]

- **Gaceta del Congreso 1023 del 02 de diciembre de 2010**

Con la finalidad de hacer aún mas palpable la importancia de dar trámite al proyecto de ley de tratamiento de datos personales, mediante la Gaceta del Congreso 1023 de 2010 se exponen los siguientes datos:

[44] Gaceta del Congreso 706 del 28 de Septiembre de 2010, página 5.

[45] Gaceta del Congreso 958 del 24 de Noviembre de 2010, página 6.

"La sociedad moderna es una palpable representación de la importancia social y económica que tiene la información, los datos y su tratamiento, así permite entenderlo las siguientes cifras: el 18% de las compañías no hacen pública su política respecto de los datos personales, el 35% elaboran perfiles de sus usuarios, en función de los cuales disponen publicidad y ofertas en sus páginas, el 86% de los servidores usan 'cookies', que registran los hábitos de consulta y otros datos de sus visitantes, el no cumplimiento de los protocolos de buenas prácticas en la protección de datos, la elaboración de perfiles de usuarios y técnicas de marketing que son cada vez más exhaustivas y se entrometen en la privacidad del usuario, las nuevas tecnologías de información aumentan caminos tendientes a erosionar el derecho a la intimidad, además del manejo no limitado y regulado la información y datos hecho por entidades del sector salud, educación, comercio y en general todos los sectores que hacen parte de la estructura social."[46]

Adicionalmente, se manda la creación de una Delegación de Protección de Datos dentro de la Superintendencia de Industria y Comercio. Igualmente, se incorpora un nuevo parágrafo al artículo 19 del proyecto de ley, en el cual se establece que el Gobierno Nacional deberá reglamentar esta materia en un plazo no superior a seis meses.

3.2.2.2. DEFINICIONES Y APLICACIÓN DEL RÉGIMEN GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

El Régimen General de Protección de Datos Personales en Colombia se encuentra regulado en la Ley 1581 de 2012 (*Por la cual se dictan disposiciones generales para la protección de datos personales*), en el Decreto 1377 de 2013 (*Por el cual se reglamenta parcialmente la Ley 1581 de 2012*) y en el Decreto 886 de 2014 (*Por el cual se reglamenta el artículo 25 de la ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos)*. Sin perjuicio de lo anterior, se observa que el Decreto 1377 de 2013 no regula en su totalidad todo aquello

[46] Gaceta del Congreso 1023 del 02 de diciembre de 2010, página 2.

contenido en la ley 1581 de 2012, muchos menos el Decreto 886 de 2014, por lo cual se hará necesario que en algún momento se desarrollen mediante otros instrumentos legales aspectos como el tratamiento de datos de niños, niñas y adolescentes, por tener un ejemplo, entre otros.

Como se expuso anteriormente, las normas citadas estipulan algunos conceptos, los cuales es necesario tener claros para poder comenzar un estudio concienzudo y sistemático del Régimen de Responsabilidad por incumplimiento de los preceptos legales de Protección de Datos Personales en Colombia:

- **Dato Personal** se debe entender "*Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"*[47]

- **Bases de Datos** el "*Conjunto organizado de datos personales que sea objeto de Tratamiento."*[48]

Sin embargo esto no es suficiente para comprender la totalidad del Régimen de Tratamiento de Datos Personales, pues así mismo la ley estipula quiénes son sujetos de derechos y obligaciones, en los siguientes términos:

- **Titular** será la "*(p)ersona natural cuyos datos personales sean objeto de Tratamiento"*[49]

[47] Ley estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, artículo 3º, Definiciones.

[48] Ley estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, artículo 3º, Definiciones.

[49] Ley estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, artículo 3º, Definiciones.

Al respecto del concepto de titular Remolina Angarita lo define como *"la persona natural cuyos derechos se requiere proteger y evitar que se lesionen o pongan en riesgo cuando su información es recolectada, almacenada o usada por parte de terceros."*[50]

- **Encargado del Tratamiento** será la ***"(****p)ersona 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** será la ***(****p)ersona 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."*[51]

De lo anterior podemos observar que la legislación colombiana no asimila la calidad de Responsable y Encargado del Tratamiento de los Datos Personales, aun cuando ambas calidades puedan confundirse eventualmente en la misma persona. Por tanto desde un inicio se observa como existen dos escenarios completamente diferenciales frente a la violación del Régimen Legal de Protección de Datos Personales. Es menester en este punto ahondar un poco más en que significa el tratamiento, pues es este un concepto técnico que no puede definirse estrictamente desde lo jurídico. En la Ley 1581 de 2012 el concepto de tratamiento hace referencia a "*cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.*"[52]

---

[50] Nelson Remolina Angarita, Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012, Primera Edición, LEGIS Editores S.A., 2013, página 113. Al respecto del concepto de titular como persona natural vale la pena traer a colación la sentencia C – 748 de 2011, Honorable Corte Constitucional de Colombia, Magistrado Ponente Jorge Ignacio Pretelt Chaljub, en la cual dicha corporación establece que "las personas jurídicas también son titulares del derecho al *habeas data*, pues como se explicó en la consideración 2.5.6.3, la protección que se brinda a las personas jurídicas en este respecto es en virtud de las personas naturales que la conforman. Por tanto, eventualmente, la protección del *habeas data* se podrá extender a las personas jurídicas cuando se afecten los derechos de las personas naturales que la conforman."

[51] Ley estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, artículo 3º, Definiciones.

[52] Ley estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, artículo 3º, Definiciones. Para ampliar la definición de Tratamiento se puede citar la Propuesta de Reglamento General de Protección de Datos del Parlamento Europeo y del Consejo – 2012: "*Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, efectuadas o no mediante procedimientos automatizados, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por*

Si lo anterior no fuera suficiente, las disposiciones legales que regulan la materia hacen, además, una clara diferenciación entre la generalidad de los datos personales y aquellos a los que denomina **Datos Sensibles**, siendo estos últimos "*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.*"[53]

A la par de los conceptos anteriormente mencionados debe además mencionarse el referente al de **Autorización**, el cual, en los términos de la ley 1581 de 2012 se entiende como "*el consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales."* [54] No está de más hacer la claridad de que, como cualquier otra manifestación de la voluntad encaminada a la creación de efectos jurídicos, está debe de ser libre, especifica, informada y libre de vicios del consentimiento en que haya podido incurrir el titular, tales como, error, fuerza o dolo.

Al hablar de autorización y considerando las particularidades que la misma debe reunir para producir efectos se hace necesario hacer un llamado a los mecanismos mediante los cuales se puede manifestar dicha Autorización, siendo el principal y mas importante el contrato, considerando este como la herramienta idónea para la regulación del tratamiento de datos personales en el comercio electrónico. El contrato, como fenómeno jurídico es el vehículo idóneo para que las entidades, de naturaleza pública o privada, PYMES o multinacionales, o quien sea, acceda a la autorización de un titular de derechos para el tratamiento de sus datos personales. Este contrato, por medio del cual se adquiere una autorización, suele conocerse

transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, supresión o destrucción."

[53] Ley estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, artículo 5º, Datos Sensibles.

[54] Ley estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, artículo 3, Definiciones.

como Electronic Data Interchange -EDI-, documento por medio del cual dos o más personas fijan las pautas sobre el tratamiento de datos personales.

> "*Mediante los acuerdos EDI se pactan las reglas de intercambio electrónico de datos bajo pautas técnicas y jurídicas previamente convenidas entre los participantes de un sistema de información y reguladas por códigos o acuerdos de dicha naturaleza."*[55]

Actualmente, y en respuesta a la imposición de un mundo globalizado en las relaciones jurídico comerciales, se ha hecho común que estos contratos en virtud de los cuales se adquiere la autorización para el tratamiento de datos personales migren a ser menos negociados por las partes, convirtiéndose, invariablemente, en contratos de adhesión, en los cuales la parte que brinda su autorización no cuenta con margen de negociación, produciendo los problemas consecuentes en el ordenamiento jurídico.[56]

Finalmente, como documentos adicionales resultantes de la expedición de la Ley 1581 de 2012, se deben nombrar los siguientes:

- **Política de Tratamiento de la Información** – PTI

Respecto de tal concepto no existe una definición legal contenida en la Ley 1581 de 2012 o en el Decreto 1377 de 2013, sin embargo es un concepto que es nombrado en múltiples

[55] Nelson Remolina Angarita, Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012, Primera Edición, Legis, 2013, página 23.

[56] Al respecto de los contratos por adhesión, se expresa por Guillermo Ospina Fernández y por Eduardo Ospina Acosta en su libro Teoría General del Contrato y del Negocio Jurídico que *"(l)as características especiales del contrato por adhesión han inducido a varios tratadistas del derecho público y a unos pocos civilistas a negar su índole contractual. Para ellos, el llamado contrato por adhesión es un acto jurídico unilateral en que "el único y verdadero agente", generalmente una poderosa empresa, al emitir una "voluntad reglamentaria", impone su decisión a otra persona que, por consiguiente, solo desempeña un papel pasivo en la operación. Pero la gran mayoría de los tratadistas de derecho civil rechaza esta concepción artificiosa, con fundamento en que la ley, en parte alguna, exige que la formación del contrato sea la culminación de un proceso de discusión entre los agentes. Como dice Josserand, ni la igualdad económica ni la igualdad verbal son condiciones necesarias para la validez de los contratos; basta con la igualdad jurídica*." Teoría General del Contrato y del Negocio Jurídico, TEMIS, Bogotá, Colombia, 2009, página 68.

ocasiones en dichas normativas. De la lectura de ambas puede concluirse que la PTI es un manual interno de políticas y procedimientos que se establecen con el fin de garantizar el debido cumplimiento de las disposiciones legales en tratamiento de datos personales.[57] Al respecto de la PTI Remolina Angarita concluye que la misma es de obligatoria adopción y cumplimiento por parte de los Responsables y Encargados del Tratamiento de los Datos Personales, y que darla a conocer a los Titulares de los Datos Personales es igualmente su responsabilidad.

- **Aviso de Privacidad**

Respecto de este concepto, se puede encontrar en el artículo 15 del Decreto 1377 de 2013 y su importancia radica, principalmente, en la manifestación que se debe hacer al titular de los datos de las políticas de tratamiento que le serán aplicadas. Así pues, la norma citada expresa que el aviso de privacidad será:

> "*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.*[58]
>
> *El aviso de privacidad, como mínimo, deberá contener la siguiente información:*
>
> 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.*

[57] La existencia de las PTI se ve íntimamente ligada con el principio de transparencia que debe existir en las legislaciones que regulen el tratamiento de Datos Personales, así pues, la resolución de Madrid de 2009 establece que la transparencia se traduce en que el responsable del tratamiento de Datos Personales cuente con *"Políticas transparentes en lo que a los tratamientos de datos de carácter personal que realice se refiere."*

[58] Decreto 1377 de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012, artículo 3º, numeral 1º.

3. Los derechos que le asisten al titular.

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.

No obstante lo anterior, cuando se recolecten datos personales sensibles, el aviso de privacidad deberá 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, de conformidad con lo establecido en este decreto."[59]

Aunado a las categorías de tratamiento de datos personales, observamos como el abanico de posibilidades de incumplimiento de estos se amplía cada vez más, ¿quiere decir eso entonces que todos los datos que se recolecten en Colombia son susceptibles de la aplicación de estas disposiciones? Lo correcto es decir que no, pues aunque el legislador desarrollo categorías especiales dentro de la Ley 1581 de 2012, igualmente estableció regímenes especiales excluidos, los cuales son:

- Bases de datos de naturaleza doméstica
- Bases de datos de Seguridad y Defensa Nacional
- Bases de datos de Inteligencia y Contrainteligencia
- Bases de datos periodísticas y de contenidos editoriales
- Bases de datos del sector financiero

[59] Decreto 1377 de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012, artículo 15.

– Bases de datos del Censo de Población y Vivienda[60]

Previa la inmersión en el régimen de responsabilidad por la violación de las disposiciones de protección de datos personales en Colombia y sus respectivas sanciones, aplicables en virtud de la potestad sancionatoria de la Administración, debe llamarse la atención sobre el análisis económico del fenómeno estudiado en el presente documento. Así pues, no está de más advertir sobre el hecho de que los datos personales, individualmente considerados, y como se expresó en el dictamen preliminar *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, el Supervisor Europeo de Protección de Datos (SEPD) son "el petróleo de la economía digital"[61], con lo cual debe de surgir la pregunta ¿qué se puede hacer a gran escala con estos datos? ¿Hacia dónde se dirige el fenómeno? Para responder estas preguntas debe de tenerse inicialmente claridad sobre los conceptos de *Big Data* y *Analytics.*

- *Big Data*: conjunto de datos personales cuyo análisis se encuentra más allá de las habilidades típicas de los software para su captura, almacenaje y análisis.[62]

- *Analytics*: Es el proceso, generalmente complejo, en virtud del cual se analiza un conjunto masivo y variado de datos con el fin de descubrir información oculta, como son patrones, correlaciones desconocidas, tendencias de mercado y preferencias de

[60] Ley estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, artículo 2º, Ámbito de Aplicación.
[61] European Data Protection Supervisor, Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, Bruselas, marzo 2014. Consultado en https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf en octubre de 2019.

[62] European Data Protection Supervisor, Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, Bruselas, marzo 2014, página 6. "Big data 'refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed using computer algorithms'; Article 29 Working Party, Opinion 03/2013 on purpose limitation, p. 35. According to an alternative definition, big data means 'datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyse'; McKinsey Global Institute, 'Big data: The next frontier for innovation, competition, and productivity', June 2011. In this preliminary Opinion 'big data' is used as shorthand for the combination of massive personal data collection and analytics on high variety, high volume datasets." Consultado en https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf el 30 de octubre de 2019.

los consumidores, lo cual se lleva a cabo con el fin de tomar decisiones de negocio informadas.[63]

Comprendidos estos conceptos, por más escuetamente legales que sean, se puede entender entonces la posición expuesta por Recio Gayo cuando expresa "*Vistos como una revolución, los datos masivos y la analítica computacional (analytics) están en plena expansión ascendente y no tienen fronteras."*[64] Por lo anterior y por la importancia de la recolección y debida administración de datos, es que la Comisión Europea estimaba y esperaba que los servicios de tecnología y *Big Data* representaran un valor mundial de 16.900 Millones USD para el año 2015.

Sin perjuicio de lo anterior debe llamarse la atención sobre el hecho de que no todos los análisis que se han hecho respecto del tratamiento de datos personales a nivel macro son perjudiciales, muy por el contrario. Como lo expresa Recio Gayo "(*a)l respecto, la International Conference of Data Protection and Privacy Commissioners (ICDPPC) en su Resolución sobre big data ha indicado:*

> *"Se afirma con frecuencia que la capacidad de almacenar y analizar grandes cantidades de datos puede ser benéfica para la sociedad. El big data (metadatos) puede utilizarse, por ejemplo, para predecir la propagación de epidemias, descubrir los graves efectos secundarios de medicamentos y combatir la contaminación en las grandes ciudades."*[65]

Por todo lo anteriormente expuesto, es decir, derivado de la importancia del tratamiento de datos personales, la existencia de fenómenos como el *Big Data* y su correspondiente análisis,

---

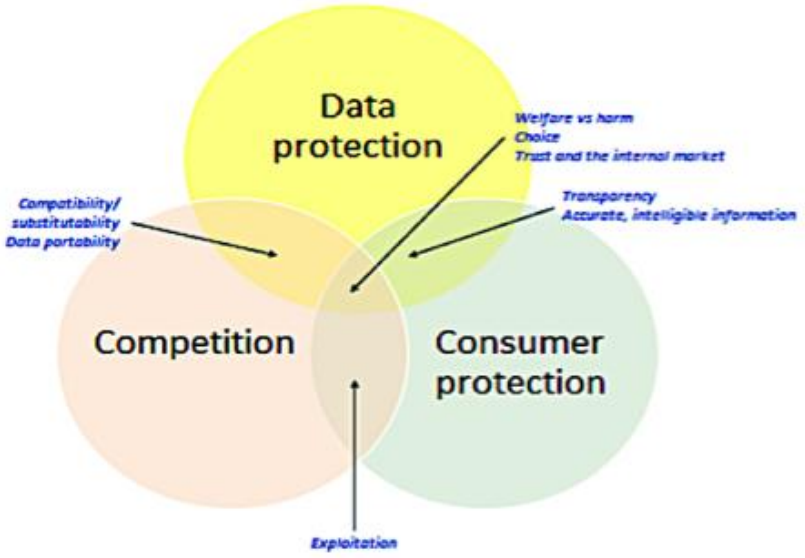
[63] Consultado en https://searchbusinessanalytics.techtarget.com/definition/big-data-analytics en octubre de 2019.

[64] Miguel Recio Gayo, Big Data: Hacia la protección de Datos Personales basada en una transparencia y responsabilidad aumentadas, Revista de Derecho, Comunicaciones y Nuevas Tecnologías, Universidad de los Andes, Facultad de Derecho, No. 17, enero – junio 2017.

[65] Miguel Recio Gayo, Big Data: Hacia la protección de Datos Personales basada en una transparencia y responsabilidad aumentadas, Revista de Derecho, Comunicaciones y Nuevas Tecnologías, Universidad de los Andes, Facultad de Derecho, No. 17, enero – junio 2017, página 4.

el acceso de grandes corporaciones y entidades a conjuntos masivos de datos en virtud de la globalización y la creciente dificultad de regular por parte del Estado la recolección, administración, protección y disposición de estos, es que debe preguntarse cual es el mejor sistema de responsabilidad y que tan eficiente es el Sistema de Protección de Datos en Colombia colombiano cuando se le compara con sistemas extranjeros y supranacionales.

> *"En el caso de la persona física a la que se refieren los datos, ya no es una mera cuestión de consentimiento, legitimación o licenciamiento para el uso o explotación de los datos recolectados y analizados, sino de garantizar la responsabilidad (accountability) a lo largo de toda la cadena de tratamiento de los datos masivos y hacerlo de manera transparente, cuando se trate de sus datos personales."*[66]



[67]

4. PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA EN EL SISTEMA DE PROTECCIÓN DE DATOS PERSONALES

[66] Miguel Recio Gayo, Big Data: Hacia la protección de Datos Personales basada en una transparencia y responsabilidad aumentadas, Revista de Derecho, Comunicaciones y Nuevas Tecnologías, Universidad de los Andes, Facultad de Derecho, No. 17, enero – junio 2017, página 5.

[67] European Data Protection Supervisor, Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, Bruselas, marzo 2014, página 2.

Previo el estudio de la aplicación del principio de Responsabilidad Demostrada por la violación de las disposiciones legales del Sistema de Protección de Datos Personales es menester entender qué es la Responsabilidad Demostrada. Así pues, la Superintendencia de Industria y Comercio, en su documento denominado *Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability)* ha expresado:

> *"El concepto de responsabilidad demostrada aplicada al tratamiento de datos personales tiene más de 30 años. Y en 1980, las Guías para la protección de la privacidad y los flujos transfronterizos de datos personales introdujeron el concepto, conocido en inglés como accountability, donde se enfatizaba el rol del Responsable de Tratamiento como el llamado a implementar medidas dentro de la organización que le permitieran cumplir con el resto de principios consagrados por dicho instrumento"*[68]

Sin embargo, el anterior concepto de la Superintendencia de Industria y Comercio no responde el interrogante, ¿qué es la Responsabilidad Demostrada? Dejando únicamente claro que dicho principio es de obligatoria implementación por el Responsable de Tratamiento de los Datos Personales.

4.1. ÁMBITO INTERNACIONAL

El principio de Responsabilidad Demostrada en relación con el tratamiento de datos personales ha tenido un desarrollo internacional en varios países del primer mundo, y para entender debidamente el funcionamiento del mismo se puede referir al seno de la OCDE, en el cual se han dado gran parte de los importantes avances en asuntos relacionados con el debido tratamiento de estos. Así pues, en la página web de la OCDE se expresa que el desarrollo del procesamiento automático de datos, el cual permite la transmisión de una gran cantidad en segundos a través de fronteras nacionales e incluso continentales, ha hecho

[68] Superintendencia de Industria y Comercio, Guía para la implementación del principio de Responsabilidad Demostrada (Accountability), Bogotá D.C., Colombia, página 4. Consultado en https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf en noviembre de 2019.

necesario considerar la protección de la privacidad en relación con los datos personales. Estas cavilaciones a niveles internacionales tienen como fin prevenir aquello que es considerado como una violación a derechos humanos fundamentales[69], violaciones tales como el almacenamiento ilegal de datos personales, el almacenamiento erróneo de datos personales o el abuso en la exposición de tales datos.[70]

Dado lo anterior, y con el fin de desarrollar un marco ideal de protección de datos personales para los miembros de la comunidad internacional, es que la OCDE en su documento *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* establece que el principio de Responsabilidad Demostrada implica que el Responsable del Tratamiento de los Datos Personales será garante en acatar las medidas necesarias para la implementación total de los principios listados en el documento[71], es decir:

- **Principio de límite en la recolección de información**: el cual implica un límite en la recolección de la información personal que puede realizarse. Advierte igualmente

[69] Vale la pena llamar la atención sobre este punto, toda vez que como se observa, para la OCDE la protección de Datos Personales tiene el carácter de un Derecho Humano, alineándose así con la posición europea, y alejándose de la posición estadounidense que le considera un derecho del consumidor.

[70] Para mayor información consultar OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Preface en la página web https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Consultado en noviembre de 2019. *"The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data (...) On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance."*

[71] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Basic Principles of National Application – Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above. https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Consultado en noviembre de 2019.

que la recolección debe de realizarse por medios legales y, en la medida de lo posible, con el conocimiento del sujeto.[72]

- **Principio de calidad de la información**: la información personal recolectada debe ser relevante para el fin para el cual se recolecta, lo cual implica que debe ser certera, completa y actualizada.[73]

- **Principio de especificación**: la finalidad con la cual es recolectada la información por parte del Responsable de Tratamiento debe de ponerse en conocimiento del propietario de la información de la manera anterior al acto de la recolección.[74]

- **Principio de limitación**: la información personal que haya sido recolectada debe ser usada dentro de los límites especificados anteriormente, excepto en los eventos en los cuales medie autorización del sujeto propietario de la información o por mandato de la autoridad o la ley.[75]

[72] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Basic Principles of National Application – Collection Limitation Principle - https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Consultado en noviembre de 2019.

[73] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Basic Principles of National Application – Data Quality Principle - https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Consultado en noviembre de 2019.

[74] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Basic Principles of National Application – Purpose Specification Principle - https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Consultado en noviembre de 2019.

[75] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Basic Principles of National Application – Use Limitation Principle - https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Consultado en noviembre de 2019.

- **Principio de salvaguardas de seguridad**: la información recolectada debe tener salvaguardas contra riesgos como son: su pérdida, acceso no autorizado, destrucción, uso indebido, modificación o revelación de la información por y hacia terceros.[76]

- **Principio de apertura**: debe existir una política de apertura sobre los desarrollos, prácticas y políticas que se apliquen respecto de los datos personales que sean recolectados. [77]

- **Principio de participación del individuo**: el individuo respecto del cual se recolecta la información deberá tener los siguientes derechos: i) el derecho a conocer si un Responsable de Tratamiento de Datos tiene en su poder información que haga referencia al individuo; ii) que se le informe, en un tiempo razonable, a un precio razonable y por un medio entendible, que información se tiene de él o ella; iii) a que se le de una razón adecuada si cualquier solicitud realizada en virtud de los numerales i) y ii) es denegada; y iv) a que su información sea borrada, rectificada, complementada o enmendada de ser procedente. [78]

En otras palabras, el principio de Responsabilidad Demostrada implica que el Responsable de Tratamiento de los Datos Personales está llamado a responder por la inobservancia de los principios anteriormente mencionados, lo cual encuentra su razón de ser en el hecho de que es aquel quién decide respecto del uso y procesamiento de los datos personales recolectados, y es en su beneficio que se realizan dichas actividades. Así pues, en atención a los pronunciamientos de la OCDE, es necesario que a la luz del ordenamiento jurídico nacional

[76] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Basic Principles of National Application – Security Safeguards Principle - https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Consultado en noviembre de 2019.
[77] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Basic Principles of National Application – Openness Principle - https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Consultado en noviembre de 2019.
[78] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Basic Principles of National Application – Individual Participation Principle - https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Consultado en noviembre de 2019.

se dé la implementación al Principio de Responsabilidad Demostrada por infracción a las disposiciones de protección de datos personales y que el Responsable del Tratamiento no pueda alejarse de la responsabilidad por el mero hecho que el procesamiento de la información sea llevado a cabo por un tercero. Adicionalmente, aclara la OCDE en su documento *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, que el mencionado principio no implica que terceros no puedan ser tenidos como responsables por incumplimiento de las disposiciones de protección de datos personales, tanto es así que, en determinadas circunstancias, puede hacerse responsable a todos los implicados, y no exclusivamente al Responsable de Tratamiento de los Datos Personales o sus contratistas, por brechas en las obligaciones de confidencialidad.[79]

Previo el estudio nacional de la aplicación del principio de Responsabilidad Demostrada cabe mencionar la multiplicidad de instrumentos que la legislación internacional han dado desarrollo a este principio, entre los que se pueden mencionar la Ley de Protección de la Información Personal y Documentos Electrónicos de Canadá, la Directiva 95/46/CE[80], Reglas de Privacidad Transfronteriza de APEC, procedimiento de *Safe Harbor* acordado entre Estados Unidos de América y la Unión Europea[81] y los Estándares de Madrid de 2009 y de Protección de Datos para los estados Iberoamericanos.

4.2. ÁMBITO NACIONAL Y DECRETO 1377 DE 27 DE JUNIO DE 2013

Una vez comprendida la conceptualización del principio de Responsabilidad Demostrada en el ámbito internacional es necesario analizar la manera en la cual el mismo es aplicado en el ordenamiento jurídico colombiano. Lo anterior entra en efectiva implementación mediante el Artículo 26 del Decreto 1377 de 2013, el cual expone lo siguiente:

[79] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Basic Principles of National Application –The Guidelines – B. Detailed Comments – Paragraph 14: Accountability Principle- https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Consultado en noviembre de 2019.

[80] Derogada por el Reglamento (UE) 2016/679 del Departamento Europeo y del Consejo.

[81] En 2015, la Decisión 2000/520/CE, de la Comisión Europea, de 26 de julio de 2000 fue anulada por el Tribunal de Justicia de la Unión Europea en la sentencia referida al Caso Schrems (C-362/14).

> *"**Articulo 26. Demostración.** Los Responsables del Tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este Decreto, en una manera que sea proporcional a lo siguiente:*
>
> 1. *La naturaleza jurídica del Responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.*
> 2. *La naturaleza de los datos personales objeto del Tratamiento.*
> 3. *El tipo de Tratamiento.*
> 4. *Los riesgos potenciales que el referido Tratamiento podrían causar sobre los derechos de los Titulares".*

Lo primero que debe preguntarse al leer la norma es, ¿cuáles son entonces las obligaciones contempladas en la ley 1581 de 2012? Como respuesta se deben cumplir los principios establecidos en el artículo 4º de la norma traída a colación (legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad), sin embargo allí no se agotan las obligaciones a la luz del principio de Responsabilidad Demostrada, pues los artículos 17 y 18 de la ley 1581 de 2012 contienen los deberes de los Responsables y Encargados del Tratamiento, respectivamente. Adicionalmente, no está de más aclarar que tales sujetos no solo deberán cumplir las disposiciones anteriormente mencionadas, sino también respetar los derechos de los titulares (artículo 8º de la ley 1581 de 2012) y dar cumplimiento a todas las disposiciones legales particulares que rijan su actividad.

Continuando con el artículo 26 del Decreto 1377 de 27 de junio de 2013, este expresa:

> *"En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como*

también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso.

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas."[82]

Por todo lo anteriormente expuesto en el presente acápite, y aunado al capítulo segundo del mismo, se puede comprender porque es la Superintendencia de Industria y Comercio la entidad llamada a decidir sobre las infracciones a las disposiciones legales en materia de protección de datos personales, especialmente a la luz del artículo 19 de la Ley 1581 de 2012.

"La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley."[83]

Finalmente, con miras a poder agotar en debidamente la aplicación nacional del principio de Responsabilidad Demostrada, se trae a colación el artículo 27 del Decreto 1377 de 2013, el cual expresa que:

***"Articulo 27. Políticas internas efectivas**. En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar:*

[82] Decreto 1377 de 27 de junio de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012, artículo 26, Demostración.

[83] Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, Artículo 19, Autoridad en Protección de Datos.

1. *La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del Responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este Decreto.*
2. *La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.*

3. *La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del Tratamiento.*

La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto".[84]

5. APLICACIÓN DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA POR LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO FRENTE AL TRATAMIENTO DE DATOS PERSONALES.

Tras la debida contextualización respecto del principio de Responsabilidad Demostrada realizada en el acápite anterior, debe explicarse ahora cuáles son los criterios de aplicación por parte de la Superintendencia de Industria y Comercio. Su empleo se verá entonces ligado a la consideración que realice respecto del Responsable del Tratamiento de los Datos Personales, pues deberá de tenerse en cuenta la existencia de medidas y políticas adecuadas en el momento de evaluar la imposición de una sanción.

[84] Decreto 1377 de 27 de junio de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012, artículo 27, Políticas internas efectivas

Lo anterior, por cuanto la norma, como se pudo apreciar, establece de manera clara e inequívoca que las medidas sancionatorias se adoptarán teniendo en cuenta todos los diversos factores que son propios a cada organización, llámese empresa o sociedad, entre los cuales resaltan variables como son el tamaño de la misma o su naturaleza jurídica, la naturaleza de los datos que se recolecten y a los que se les de tratamiento, el tipo de manejo al cual se sometan los datos y la información, y los riesgos que existan para los titulares la recolección de los datos, su uso y circulación.

Como expresa la Superintendencia de Industria y Comercio en su documento denominado *Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability):*

> *"Tal y como sucede con el modelo recogido en el decreto (1377 de 2013), y en los mismo términos en que la Superintendencia de Industria y Comercio ha venido diseñando su sistema de supervisión, el énfasis de la comunidad dedicada a la protección de la información personal tiende a volcarse hacia un modelo que privilegia la gestión del riesgo y la asignación de responsabilidades en cabeza del Responsable de Tratamiento"*[85]

5.1. BENEFICIOS QUE TRAE CONSIGO LA IMPLEMENTACIÓN DEL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

Como se expresó anteriormente, el modelo por el cual apuesta la Superintendencia de Industria y Comercio, así como las directrices internacionales, es un modelo de protección preventiva, y en ese orden de ideas es que el principio de Responsabilidad Demostrada, cuando se le da un debido cumplimiento, permite la implementación de elevados estándares de protección de datos, generando un estado de bienestar tanto para la organización que le da

[85] Superintendencia de Industria y Comercio, Guía para la implementación del principio de Responsabilidad Demostrada (Accountability), Bogotá D.C., Colombia, página 6. Consultado en https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf en noviembre 2019.

cumplimiento, como para los individuos cuyos datos personales se recolectan, usan y procesan.

La situación anterior se aprecia, específicamente, en estudiar el último inciso del artículo 27 del decreto 1377 de 2013 citado con anterioridad y que debe traerse a colación nuevamente, pues expresa que la "*La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto."*[86]

Por lo anterior, se observa que los beneficios de la aplicación del principio de Responsabilidad Demostrada pueden dividirse en beneficios a *priori* y beneficios a *posteriori*, y que actúan de manera diferente respecto del vigilado, el vigilante y el titular de los datos.

5.1.1. *A PRIORI*

5.1.1.1. EL VIGILANTE – SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO:

Teniendo en cuenta que los recursos de este sujeto son limitados, su observancia debe ser eficientemente repartida en aquellas entidades que más lo necesiten y en las cuales una brecha en el cumplimiento de los preceptos legales de protección de datos implique un riesgo sistémico, por lo cual la implementación del principio de Responsabilidad Demostrada por mandato legal permite enfocar los esfuerzos de vigilancia donde más sean necesarios.

5.1.1.2. EL VIGILADO:

Desde una perspectiva eminentemente económica y empresarial, el cumplimiento del estándar impuesto por la Ley 1581 de 2012 y por el Decreto 1377 de 2013, es beneficiosa

[86] Decreto 1377 de 27 de junio de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012, artículo 27, Políticas internas efectivas.

para la organización vigilada toda vez que implica un beneficio reputacional[87] en un momento de la historia en los cuales los valores como la transparencia, la honestidad, la atención al cliente y la globalización de la información son fundamentales para las relaciones comerciales y la supervivencia en el mercado. Igualmente, mediante la implementación de un sistema de protección de datos que cumpla con los requerimientos del principio de Responsabilidad Demostrada, se observa una disminución en los riesgos de violación de las disposiciones legales.

5.1.1.3. EL TITULAR DE LOS DATOS:

Para el titular de los datos personales recolectados, usados y/o procesados la implementación del principio de Responsabilidad Demostrada representa unos beneficios a *priori* en la medida en que conocerá de forma inequívoca sus derechos respecto de sus datos, su facultad de solicitar actualizaciones, supresiones, información adicional, que se le explique con qué fin se están recolectando los datos, quienes utilizarán los mismos, quien es el Responsable y el Encargado de Tratamiento, si son la misma persona o sin diferentes, entre otras situaciones que son de necesario conocimiento con el fin de que se ejerza en debidamente el derecho al *Habeas Data.*

5.1.2. A POSTERIORI

5.1.2.1. EL VIGILANTE – SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO:

Haber implementado un sistema que cumpla con las especificidades del principio de Responsabilidad Demostrada representará un beneficio para el vigilante toda vez que tendrá

[87] El concepto del riesgo reputacional es un concepto eminentemente administrativo y empresarial, que sin embargo ha permeado en los últimos años profesiones como la publicidad, el marketing, la contabilidad, las finanzas e incluso el derecho. El riesgo reputacional, de acuerdo al documento publicado por Deloitte y denominado Global Survey on Reputational Risk, es la posibilidad de que la percepción de terceros y accionistas de una sociedad respecto de la misma sea perjudicada por acciones de la misma, mermando así su valor en el mercado y poniendo en riesgo sus relaciones comerciales con clientes y proveedores. Para mas información consultar https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/NEWReputationRiskSurveyReport_25FEB.pdf. Consultado en Noviembre de 2019.
De acuerdo a un estudio adelantado por el World Economic Forum en 2012, es estimado que más del 25% del valor en mercado de una compañía depende directamente de su reputación. Para mas información consultar World Economic Forum, 2012.

un marco preexistente que en el cual basar su decisión sancionatoria por el incumplimiento de las disposiciones legales en materia de protección de datos personales.

5.1.2.2. EL VIGILADO:

Para la organización vigilada los beneficios a *posteriori* se observan al leer el inciso final del artículo 27 del Decreto 1377 de 2013, el cual se ha citado en oportunidades anteriores y que prevé que la existencia de un sistema de protección de datos recolectados por parte de una organización deberá ser tenido en cuenta por parte de la Superintendencia de Industria y Comercio para la imposición de sanciones por la violación de las normas que rigen la actividad de recolección, uso, almacenamiento y procesamiento de datos personales.

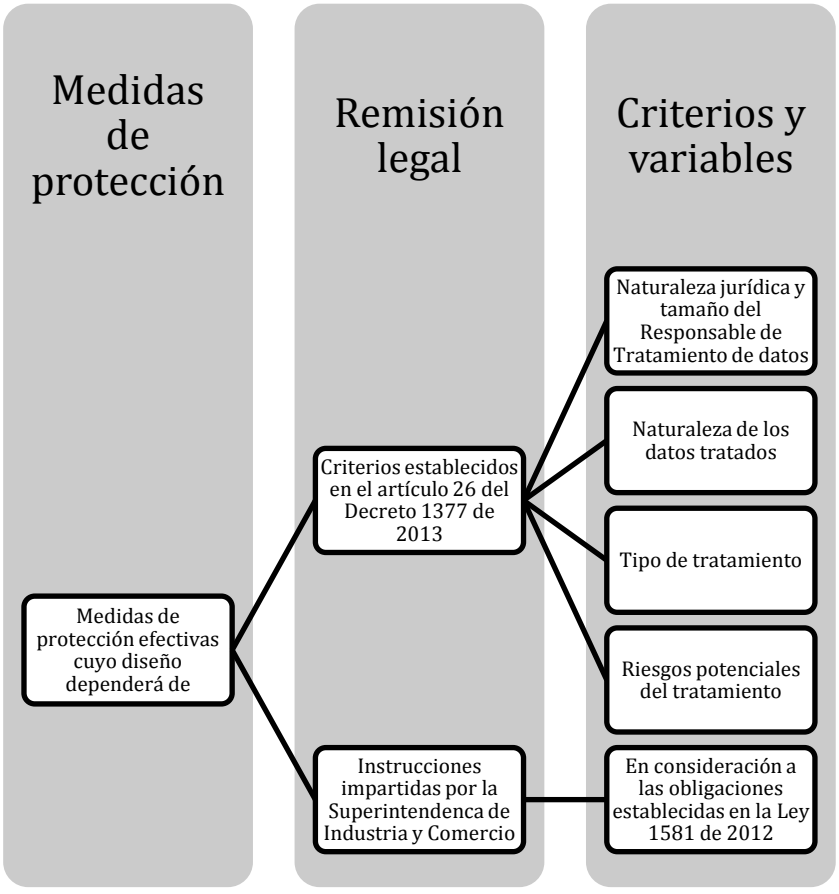
5.1.2.3. EL TITULAR DE LOS DATOS:

De manera posterior a la recolección de datos y al incumplimiento de los preceptos legales por parte de la organización, el beneficio que se presenta para el titular de los datos es que conocerá el marco en el cual se presentó la recolección, el uso, la transferencia, el análisis y/o procesamientos indebido de sus datos, pudiendo, de esta manera exigir el cumplimiento de estos.

5.2. VARIANTES Y FACTORES INCISIVOS EN LAS DECISIONES ADMINISTRATIVAS SANCIONATORIAS ADOPTADAS POR LA SIC, FRENTE AL INCUMPLIMIENTO DE LOS DEBERES ESTABLECIDOS EN EL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES

Tras el procedente análisis de la norma y la forma debida en la cual se debe dar implementación al principio de Responsabilidad Demostrada por parte del Responsable y/o Encargado del Tratamiento de los Datos Personales es apenas natural preguntarse cuáles son, de acuerdo a la norma, aquellas variables y factores a los que hace alusión el artículo 27 del Decreto 1377 de 2013 al expresar que la Superintendencia de Industria y Comercio tendrá en consideración la existencia de medidas y políticas para la imposición de sanciones por la violación de las disposiciones legales.

Sin perjuicio de lo anterior, se observa que la situación explicativa no se podría agotar con una lista enunciativa de variantes y factores, por el contrario, estas mismas características se encuentran determinadas por una serie de variables. Esto implica, así mismo, que la sanción administrativa dependerá de que la organización haya implementado medidas efectivas de protección de datos personales; dichas medidas a su vez deberán ser diseñadas en consideración a los numerales 1, 2, 3 y 4 del artículo 26 del Decreto 1377 de 2013 y a las instrucciones impartidas por la Superintendencia de Industria y Comercio, todo lo cual deberá, en ultimas, de respetar las obligaciones contenidas en la Ley 1581 de 2012.



88

Finalmente, expresa la norma citada, que dichas políticas de protección de Datos Personales deberán de garantizar:

[88] Diseño de elaboración propia.

- La existencia de una estructura administrativa que sea proporcional a la estructura y tamaño empresarial del Responsable de Tratamiento de Datos.

- La adopción de mecanismo que permitan dar aplicación eficiente y en tiempo real de las políticas de protección de datos personales, esto mediante herramientas de implementación, entrenamiento y programas de educación.

- La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares con respecto a cualquier aspecto del tratamiento de datos personales.[89]

Por lo anterior se puede concluir que las variantes y factores que influyen en la decisión administrativa de la Superintendencia de Industria y Comercio para la imposición de sanciones por violación a las disposiciones de protección de datos personales son de carácter puramente legal, pero observando los mismos bajo una óptica de eficiencia en el ejercicio de los derechos ya que, como menciona la norma, el diseño institucional de la política de tratamiento de datos de personales en cada organización dependerá de factores puntuales y dinámicos, que irán cambiando con el paso del tiempo, y que por tanto harán necesario la variación y dinamismo de dichas políticas.

5.3. CRITERIOS DE LA SIC AL APLICAR SANCIONES POR VIOLACIONES AL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

Finalmente, con el fin de comprender la materialización del principio de Responsabilidad Demostrada por violaciones a la protección de datos personales es menester analizar la forma en la cual da aplicación la Superintendencia de Industria y Comercio al mismo. Tras un análisis de las diferentes resoluciones emanadas de dicho organismo puede concluirse que basa sus criterios de sanción por la violación de los derechos de los titulares, derechos que se encuentran en el artículo 8º de la Ley 1581 de 2012.

[89] Decreto 1377 de 27 de junio de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012, artículo 27, Políticas internas efectivas.

Entre las resoluciones emitidas por parte de dicha autoridad vale la pena traer a colación aquellas que hagan referencia a las siguientes disposiciones legales en los casos en que son inobservadas:

5.3.1. TRAMITAR CONSULTAS Y RECLAMACIONES EN EL TÉRMINO LEGAL ESTABLECIDO

De acuerdo a diferentes pronunciamientos de la Superintendencia de Industria y Comercio a través de sus resoluciones, ha mencionado que el derecho a que se tramiten las consultas y reclamaciones en el término legal establecido se encuentra íntimamente ligado con el derecho de petición, circunstancia estudiada por la Honorable Corte Constitucional y que al respecto se pronunció mediante la sentencia C – 748 de 2011 en la que explica:

> *"Los artículos 14 y 15 del proyecto de ley regulan los mecanismos de consulta y reclamo del titular del dato o sus causahabientes al responsable o encargado del tratamiento, con el fin de hacer efectivo el derecho al habeas data. Se señala que: (i) los titulares o sus causahabientes podrá consultar la información personal de titular que repose en cualquier base de datos pública o privada; (ii) los responsables y encargados del tratamiento deben suministrar al titular toda la información contenida en la base de datos bien porque se tenga un registro individual o exista alguna asociada a su identificación; (iii) el responsable y el encargado del tratamiento deben tener algún medio habilitado para que la consulta se pueda realizar, el cual debe permitir dejar prueba de ello; (iv) la consulta se debe resolver en un término máximo de 10 días hábiles a partir de la fecha de recibo de la solicitud; (v) en el evento de no poder responderse en ese término, se le debe informar al titular sobre las razones. De todas maneras la respuesta la debe recibir dentro de los 5 días siguientes al vencimiento del primer plazo"* [90 - 91]

[90]Sentencia C – 748 de 2011, Magistrado Ponente Jorge Ignacio Pretelt Chaljub.

[91] Para mayor información consultar la Resolución 49717 del 17 de agosto de 2017, expedida por la Superintendencia de Industria y Comercio. Disponible en

De lo anterior es seguro deducir entonces que cuando la ley utiliza la palabra término, este no hace referencia única y exclusivamente a conceptos temporales, por el contrario, hace alusión a toda una serie de circunstancias que deben de agotarse al dar respuesta los responsables del tratamiento a las solicitudes de los titulares.

5.3.2. GARANTIZAR SIEMPRE Y EN TODO LUGAR EL EJERCICIO PLENO Y EFECTIVO DEL *HABEAS DATA* AL TITULAR DE LA INFORMACIÓN

En la Resolución 10975 del 19 de febrero de 2018, la Superintendencia expresó, respecto de este derecho del titular que:

> "*(E)l derecho de habeas data otorga la facultad al Titular de los datos personales de exigir acceso, corrección, adición, actualización y eliminación de su información por lo que resulta apenas evidente que los Responsables y Encargados de la información deban proceder de conformidad, implementando las medidas y procedimientos correctos, dirigidos a la protección de los datos personales y su adecuado tratamiento, garantizando al Titular de la información el libre acceso y el cumplimiento de las solicitudes que el mismo haga respecto de su información"*[92]

Con el fin de ampliar el concepto de *Habeas Data* y comprender la debida forma en que se debe garantizar su funcionamiento puede hacerse referencia a la sentencia C - 748 de 2011, en la cual la Honorable Corte Constitucional concluyó que:

> "*El derecho fundamental al habeas data es aquel que otorga la facultad al titular de datos personales de exigir a las administradoras de datos personales el*

https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/2017049717RE00000000001_31-10.pdf. Consultado en noviembre de 2019.

[92] Superintendencia de Industria y Comercio, Resolución 10975 del 19 de febrero de 2018, página 5, consultado en https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE10975-2018-Reemplazar.pdf en noviembre de 2019.

acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación a la posibilidad de divulgación, publicación o cesión de los mismos conforme a los principios que informan el proceso de administración de bases de datos"[93]

5.3.3. CONSERVAR LA INFORMACIÓN BAJO ÓPTIMAS CONDICIONES DE SEGURIDAD

Mediante Resolución 13288 del 27 de febrero de 2018 expresó la Superintendencia de Industria y Comercio que:

"*Bajo los postulados que gobiernan la disposición contenida en el literal d) del artículo 17 de la Ley 1581 de 2012, es evidente que para que se pueda extraer un juicio de responsabilidad como consecuencia de la infracción a este deber, debe demostrarse que la información personal de los Titulares fue accedida por terceros no autorizados, rompiendo con los principios de circulación restringida y de seguridad de la información."*[94]

A la luz de lo expresado entonces por la Superintendencia de Industria y Comercio, se observa una remisión directa al principio de seguridad, respecto del cual la Honorable Corte Constitucional, en sentencia C – 748 de 2011 expresó que la *"información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."*[95]

[93] Sentencia C - 748 de 2011, Magistrado Ponente Jorge Ignacio Pretelt Chaljub.

[94] Superintendencia de Industria y Comercio, Resolución 13822 del 27 de febrero de 2018, página 5, consultado en https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE13822-2018.pdf en noviembre de 2019.

[95] Sentencia C – 748 de 2011, Magistrado Ponente Jorge Ignacio Pretelt Chaljub.

5.3.4. SOLICITAR Y CONSERVAR COPIA DE LA AUTORIZACIÓN PREVIA Y EXPRESA DE LOS TITULARES PARA EL TRATAMIENTO DE DATOS

Mediante Resolución 13822 del 27 de febrero de 2018 la Superintendencia de Industria y Comercio expreso que, en consideración al artículo 15 de la Constitución Política las personas, en desarrollo de su derecho a la autodeterminación informática y al principio de libertad, son quienes de forma expresa deben de autorizar la recolección, tratamiento y uso de sus datos personales y que de esta manera estos pasen a formar parte de una base de datos.

> *"Por lo anterior, se concluye que sin la autorización previa e informada del titular, los datos personales no podrán ser registrados, divulgados, ni tratados. Sin embargo, tal prohibición no es absoluta, pues la Ley 1581 de 2012 en su artículo 10 establece los casos en los que no es necesario contar con la autorización por parte del titular, entre los cuales se encuentran los datos de naturaleza pública"*[96]

Vale la pena en este punto recordar que la excepción contemplada en el artículo 10 de la Ley 1581 de 2012 no hace referencia única y exclusivamente a los datos públicos, igualmente no necesitarán de autorización previa de tratamiento los datos que sea requeridos por una autoridad pública o administrativa en cumplimiento de sus funciones, los datos a los que se acceda en casos de urgencia médica o sanitaria, el tratamiento de información autorizado por ley para fines históricos, estadísticos o científicos.[97]

5.3.5. CONTAR CON POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES

[96] Superintendencia de Industria y Comercio, Resolución 13822 del 27 de febrero de 2018, página 5, consultado en https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE13822-2018.pdf en noviembre de 2019.

[97] Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, artículo 10, Casos en que no es necesaria la autorización.

De acuerdo al literal k) del artículo 17 de la Ley 1581 de 2012 deberá cumplir el Responsable de Tratamiento de los Datos Personales el deber de *"adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento*" de la citada ley, y en especial consideración a la atención de consultad y reclamos.

Respecto de este deber ha expresado la Superintendencia de Industria y Comercio, mediante Resolución 2136 del 28 de abril de 2017, que *"(E)n consecuencia, los responsables tienen la obligación de desarrollar las políticas para el tratamiento de los datos personales, las cuales deben constar en medio físico o electrónico y ser puestas en conocimiento de los titulares.*"[98] Según lo previsto en la circular de tal autoridad, estas políticas de tratamiento de datos personales "*deberán contener los deberes de los responsables señalados en el artículo 17 de la ley 1581 de 2012 y la información relacionada, entre otras, con la finalidad y clase de tratamiento al que serán sometidos los datos personales".*[99]

6. CONCLUSIONES

Para finalizar el presente documento, y a forma de conclusión, puede llamarse la atención respecto de ciertos puntos neurálgicos del Sistema de Protección de Datos Personales en Colombia y la aplicación del principio de Responsabilidad Demostrada.

1. En el mundo globalizado en el cual se vive hoy en día es una realidad que un sistema de protección de Datos Personales que no tome en consideración fenómenos como el *Big Data*, la transmisión transfronteriza de información, la capacidad ilimitada de procesamiento de datos personales, y las implicaciones económicas, sociológicas, ecológicas y políticas de estos fenómenos está llamado a fracasar.

[98] Superintendencia de Industria y Comercio, Resolución 2136 del 28 de abril de 2017, página 13, consultado en https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/2017021360RE0000000001.pdf en noviembre de 2019.

[99] Superintendencia de Industria y Comercio, Circular Básica Jurídica.

2. El Sistema de Protección de Datos Personales en Colombia se encuentra profundamente permeado por las directrices de la OCDE y el Sistema Europeo de Protección de Datos Personales, jurisdicciones que adicionalmente consideran el derecho al *Habeas Data* como un derecho fundamental.

3. La implementación de un sistema adecuado de protección de datos, cuyo diseño y aplicación responda a los parámetros legales, permitirá tener, a la empresa que lo realice, una serie de beneficios entre los que cabe resaltar la minimización del riesgo reputacional, la maximización de la satisfacción de sus usuarios y, eventualmente, ante un incumplimiento de la norma, la minimización de una posible sanción administrativa.

4. La imposición de sanciones administrativas por la violación al régimen de protección de Datos Personales en Colombia responde a una visión integral de los derechos de los particulares, pues desde una lectura constitucional del *Habeas Data* y sistemática de las normas que regulan su protección se comprende que todos ellos componen la integridad de un sistema equilibrado y garantista, en el cual una brecha en el cumplimiento implica un desequilibrio de los derechos del titular.

Bibliografía

- BBC Noticias. (24 de julio de 2019). *BBC Noticias*. Recuperado el Septiembre de 2019, de https://www.bbc.com/mundo/noticias-49093124
- Black, E. (2001). *IBM y el Holocausto: La alianza estratégica entre la Alemania Nazi y la corporación mas poderosa de América.* Atlantida, Estados Unidos de America.
- Comité Europeo de Protección de Datos. (s.f.). *Acerca del CEPD*. Recuperado en Octubre de 2019, de https://edpb.europa.eu/about-edpb/about-edpb_es
- Comité Europeo de Protección de Datos. (s.f.). *Comité Europeo de Protección de Datos - Data Protection*. Recuperado en Septiembre de 2019, de https://edps.europa.eu/data-protection/data-protection_en
- Congreso de la Repúbica de Colombia. (28 de Septiembre de 2010). Gaceta del Congreso 706 . *Gaceta del Congreso* . Bogotá D.C., Colombia.
- Congreso de la República de Colombia. (2013). Decreto 1377 - Por el cual se reglamenta parcialmente la Ley 1581 de 2012. *Decreto* . Bogotá D.C., Colombia.
- Congreso de la República de Colombia. (02 de diciembre de 2010). Gaceta del Congreso 1023. *Gaceta del Congreso* . Bogotá D.C., Colombia.
- Congreso de la República de Colombia. (09 de Septiembre de 2010). Gaceta del Congreso 625. *Gaceta del Congreso* . Bogotá D.C., Colombia.
- Congreso de la República de Colombia. (24 de Noviembre de 2010). Gaceta del Congreso 958. *Gaceta del Congreso* . Bogotá D.C., Colombia.
- Congreso de la República de Colombia. (2012). Ley 1581 - Por la cual se dictan disposiciones generales para la protección de datos personales. *Ley de la República de Colombia* . Bogotá D.C., Colombia.
- Cosculluela Montaner, L. (2006). *Manual de Derecho Administrativo* (Vol. I). Madrid, España: Thomson Civitas.
- Deloitte. (s.f.). *Deloitte. Global Survey on Reputational Risk.* Recuperado en Noviembre de 2019, de Deloitte. Global Survey on Reputational Risk: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/NEWReputationRiskSurveyReport_25FEB.pdf

- European Data Protection Supervisor. (2014). *Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy.* Recuperado en Octubre de 2019, de https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf
- Higuera Perez, M., & Ornelas Nuñez, L. G. (Junio de 2013). La autorregulación en materia de protección de datos personales: la vía hacia una protección global . *Revista de Derecho, Comunicación y Nuevas Tecnologías* .
- International, P. (s.f.). *A guide for policy engagement on Data Protection. The key to Data Protection* . (P. International, Productor) Recuperado en agosto de 2019, de https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf
- Judgement of the General Court , T - 161 (General Court 7 de julio de 2011).
- Laverde Álvarez, J. M. (2018). *Manual de Procedimiento Administrativo Sancionatorio.* Bogotá D.C., Colombia: Legis.
- Organización para la Cooperación y Desarrollo Económicos - OCDE. (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. (O. p. OCDE, Productor) Recuperado el Noviembre de 2019, de https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
- Ospina Acosta, E., & Ospina Fernández, G. (2009). *Teoría General del Contrato y del Negocio Jurídico.* Bogotá D.C., Colombia: TEMIS.
- Recio Gayo, M. (2017). Big Data: Hacia la protección de Datos Personales basada en una transparencia y responsabilidad aumentadas. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*.
- Remolina Angarita, N. (2013). *Tratamiento de datos personales. Aproximaciones internacionales y comentarios a la Ley 1581 de 2012.* Bogotá D.C., Colombia: Legis.
- Sentencia C - 412, Corte Constitucional de Colombia, 2015.

- Sentencia C - 089 , Corte Constitucional de Colombia 2011.
- Sentencia C - 748, Corte Constitucional de Colombia 2011.
- Sentencia C - 875, Corte Constitucional de Colombia 2011.
- Sentencia C-1011, Corte Constitucional de Colombia 2008.
- Sentencia C - 595 , Corte Constitucional de Colombia 2010.
- Sentencia C - 616 , Corte Constitucional de Colombia 2002.
- Superintendencia de Industria y Comercio . (28 de Abril de 2017). *Resolución 2136.* Recuperado en Noviembre de Noviembre, de Resolución 2136: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/2017021360RE0000000001.pdf
- Superintendencia de Industria y Comercio. (s.f.). Circular Básica Jurídica. *Circular Básica Jurídica* .
- Superintendencia de Industria y Comercio. (s.f.). *Guía para la implementación del principio de Responsabilidad Demostrada (Accountability).* Recuperado en Noviembre de 2019, de Guía para la implementación del principio de Responsabilidad Demostrada (Accountability): https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf
- Superintendencia de Industria y Comercio. (19 de Febrero de 2018). *Resolución 10975.* Recuperado en Noviembre de 2019, de Resolución 10975: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE10975-2018-Reemplazar.pdf
- Superintendencia de Industria y Comercio. (27 de Febrero de 2018). *Resolución 13822.* Recuperado en Noviembre de 2019, de Resolución 13822: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE13822-2018.pdf
- Superintendencia de Industria y Comercio. (17 de Agosto de 2017). *Resolución 49717.* Recuperado en Noviembre de 2019, de Resolución 49717: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/2017049717RE0000000001_31-10.pdf.

– Superintendencia de Industria y Comercio. (31 de Agosto de 2016). Resolución 58194. Bogotá D.C., Colombia.