LA LEY DE PROTECCIÓN DE DATOS EN COLOMBIA: SUS INICIOS Y EXAMEN DE SUS PRINCIPALES POSTULADOS

Miguel Ángel Aguilar Castañeda[1]

Resumen

La protección de datos personales ha sido un tema reciente para Colombia, por lo tanto, el mismo ha sido desarrollado de manera progresiva. Inicialmente se regularon aspectos relacionados con la recolección y circulación de la información comercial y financiera de los titulares ante las bases de datos de las centrales de riesgo. Ello con el fin de crear perfiles crediticios. Sin embargo, debido a los constantes avances tecnológicos y al uso de nuevas herramientas cibernéticas se creó la necesidad de regular en detalle aspectos relacionados con los datos personales. Por consiguiente, se dio nacimiento a la Ley 1581 de 2012, en la cual se expusieron los aspectos generales en dicha materia. En el presente artículo se hará un breve recuento de los aspectos que componen dicha norma. Así como también, se procederá a analizar aspectos como el requisito de la Autorización dentro del tratamiento de datos, el principio de Responsabilidad Demostrada (accountability) y la labor que desempeñan cada uno de los sujetos intervinientes dentro de esta relación (responsables y encargados) en aras de determinar que tan efectiva y garantista es la Ley Estatutaria 1581 de 2012 en materia de tratamiento de datos personales.

Palabras claves: Datos Personales, Datos Sensibles, Datos privados, Ley de Protección de Datos, Principio de Responsabilidad Demostrada, Superintendencia de Industria y Comercio, Tratamiento de Datos, Responsable y Encargados.

[1] Artículo Investigativo presentado como requisito parcial para optar al título de abogado por parte de Miguel Ángel Aguilar Castañeda estudiante de X semestre de Derecho de la Universidad Católica de Colombia Sede Bogotá - 2018. Bajo la dirección y supervisión de la Doctora Olenka Woolcott Asesora del Centro de Investigaciones Socio Jurídicas -CISJUC

THE LAW OF DATA PROTECTION IN COLOMBIA: ITS BEGINNINGS AND THE EXAMINATION OF ITS MAIN POSTULATES

Abstract

The protection of personal data has been a recent topic for Colombia; therefore, it has been developed progressively. Initially, aspects related to the collection and circulation of commercial and financial information of the owners was regulated before the databases of the credit bureaus. This in order to create credit profiles. However, due to the constant technological advances and the use of new cybernetic tools, the need to regulate in detail aspects related to personal data was created. Consequently, Law 1581 of 2012 was born, in which the general aspects in this matter were exposed. In the present article a brief recount of the aspects that compose this norm will be made. As well as, it will proceed to analyze aspects such as the requirement of the Authorization within the data processing, the principle of Demonstrated Responsibility (accountability) and the work performed by each of the subjects involved in this relationship (responsible and in charge) in in order to determine how effective and guaranteed the Statutory Law 1581 of 2012 is in the matter of the processing of personal data

Keywords: Personal Data, Sensitive Data, Private Data, Data Protection Law, Principle of Demonstrated Responsibility, Superintendence of Industry and Commerce, Data Processing, Responsible and Managers.

Sumario

Introducción

El artículo 15 de la Constitución Política de Colombia ha desarrollado el precepto constitucional de *Habeas Data* de la siguiente manera:

> 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. (Const.,1991, art. 15).

El mismo hace referencia al derecho que tiene toda persona de conocer, actualizar, modificar o rectificar la información que se consigne en diferentes bases de datos. De ahí que los datos que se recolecten de cada titular, deben gozar de total veracidad y exactitud, ello en pro de respetar dicha Garantía Constitucional, la cual, consagra además derechos fundamentales como al buen nombre y la intimidad personal.

Este derecho fundamental inicialmente se encontraba relacionado estrictamente con la información comercial o financiera que se recolectara de los titulares de la información en aras de efectuar perfiles crediticios y análisis de riesgos crediticios. (Ley 1266 de 2008).

Sin embargo, con ocasión a los diferentes avances tecnológicos, la presencia de nuevas tecnologías en materia de aplicaciones y en general el uso cotidiano de las herramientas tecnológicas ha obligado que las personas suministren datos especiales que por su naturaleza pueden llegar a tener la condición de sensibles o privados, como por ejemplo, datos relacionados con su nombre, apellido, direcciones, teléfonos, correos electrónicos, fotografías, huellas dactilares, ubicaciones geográficas, entre otros.

Así lo ha expresado Garriga (2004), en su libro *Tratamiento de Datos Personales y derechos fundamentales:*

> El actual desarrollo de las tecnologías de la información, hace posible recoger y almacenar, sin límite de espacio, infinidad de datos sobre un mismo individuo, realizar un auténtico catálogo de información personal sobre él y además interrelacionar todos los datos existentes sobre una misma persona, con

> independencia de que se encuentren en archivos distintos, relativos a diferentes etapas de su vida, o que estos hayan sido recogido incluso en ligares diferentes. Se puede acumular sin límite la información y recabarla en cuestión de segundos con independencia de la distancia a la que se encuentre.

Información que por el tipo y la calidad de la misma ha requerido un tratamiento especial en cuanto a su uso. Por lo tanto, se ha creado la necesidad de implementar políticas de seguridad en lo que respecta a su recolección y circulación, pues el uso indebido de dicha información puede llegar a violar garantías constitucionales e ir en contravía de la intimidad personal de los titulares.

De ahí la importancia que tienen los datos personales, pues estos resultan ser un componente significativo para la identificación de una persona. Así lo ha sostenido la Superintendencia de Industria y Comercio en su Guía *Sobre la Protección de datos personales* "Cuando hablamos de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación" (2016).

En esa medida, ante la necesidad de un tratamiento especial de los datos personales, nace en Colombia la Ley 1581 de 2012, en la cual se incluyó todas las disposiciones generales en materia de protección de datos personales y se emitieron lineamientos respecto a la recolección, manejo y circulación de todos los datos que fueran incluidos en las diferentes bases de datos.

Así las cosas, teniendo en cuenta el gran universo que abarca los datos personales, resulta importante analizar más a fondo cada uno de los parámetros establecidos en materia de protección de datos, pues ante la constante globalización respecto a las nuevas tecnologías, los datos personales se convierten en un activo de cada persona y por lo tanto, merecen una política integral sobre el uso y la destinación de los mismos. Esto con el fin de atender al principio de responsabilidad demostrada.

Conocer los fundamentos de la Ley Estatutaria 1581 de 2012 y los lineamientos que esta propone respecto a las condiciones de seguridad a las cuales deben sujetarse los datos personales, permite que como dueños de la información, cada persona haga respetar el buen uso y la correcta destinación de sus datos y de esta manera prevenir los daños derivados de un uso inadecuado de los datos personales.

Sin embargo, si bien la norma desarrolla y abarca en su totalidad todos los lineamientos necesarios, que deben ser tenidos en cuenta para crear políticas efectivas en materia de tratamiento de datos personales, con el fin de prevenir conductas inadecuadas en este proceso, la misma es carente frente a la regulación relacionada con las responsabilidades por los daños y/o perjuicios que puede acarrear un tratamiento de datos deficiente.

Así pues, la norma destinó un Título para regular todo lo relacionado a los mecanismos de vigilancia y sanción, en donde, se enuncian los tipos de sanciones frente al incumplimiento de los deberes por parte de los Responsables o Encargados del tratamiento de datos. Es decir, se estructura un modelo sancionatorio.

No obstante, frente al directo afectado, que para el caso en particular resultan ser los titulares de la información, no se reguló un resarcimiento frente a los posibles daños a los que se vieron inmersos estos, aun cuando la norma protege de manera especial al dueño de dicho activo. Es decir, se evidencia un vacío normativo, pues la Ley Estatutaria no regula de manera directa los aspectos relacionados a la reparación del perjuicio causado.

El ordenamiento a través de la promulgación de dicha norma estructuró políticas efectivas en pro de velar por el respeto y la protección a los datos personales, empero dejó de lado regular un tema relevante como lo es la Responsabilidad Civil y la reparación de daños. Un cambio relevante que ha implementado el Derecho Privado en estos temas tal y como lo ha expresado Woolcot et al. (2018).

Con todo ello, vale la pena resaltar los avances que se lograron con la expedición de dicha norma, pues la misma, obligó que todo el tratamiento de datos personales estuviera directamente relacionado con la protección de garantías constitucionales. Así mismo, obligó a todas las empresas que recolectan datos y en general para todos aquellos sujetos que administran estas bases, estructurar políticas de seguridad que se encuentren acorde a los lineamientos legales y evite de esta manera el riesgo que puede generar para los derechos y libertades de una persona el manejo inadecuado de los datos.

1. Datos Personales

1.1 Concepto de Datos Personales a nivel general

Los Datos personales son aquellos que permiten identificar a una persona, como, por ejemplo, datos referentes al nombre, apellido, número de cédula, entre otros. Así mismo, los datos personales están directamente relacionados con el titular, como es el caso del número de celular, dirección etc.

En ese sentido lo ha definido la Comisión Europea "Los datos personales son cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal." (2018)

Adicional a ello, con ocasión a los constante cambios tecnológicos, dichos datos personales se han vuelto activos de constante circulación y por lo cual, requieren de una protección especial. Así lo han dicho Soto y Ducura (2018)

> la información de tipo personal que se procesa en internet puede identificar o hacer identificable a una persona en particular, puesto que se incluye información de tipo identificación como nombre, dirección, teléfono, fotografías; entre otras, de ahí la importancia de la protección de esa información en ámbitos intangibles como lo es internet o como es conocido hoy en día el ciberespacio. (Soto y Ducura, 2018, p.27)

La Ley 1581 de 2012 ha señalado que el Dato personal es "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables". (Ley 1581, 2012, art.3 literal c)

Se tiene entonces que los datos personales son aquellos que poseen información específica de una persona y por tanto, los mismos permiten una vinculación y una asociación directa con ésta.

Ahora bien, es importante precisar que los datos personales son recolectados por diversas vías, de ahí que se logre obtener un cumulo de información de todo tipo. Por lo tanto, en el

proceso de recolección y administración de información, resulta necesario hacer una segmentación de dicha información e identificar la naturaleza de cada dato; de tal manera que por su condición de privado, semiprivado, sensible o público, el tratamiento de los mismos sea más eficaz y respete las garantías constitucionales que tiene cada titular de dicha información. Ello en aras de salvaguardar derechos como lo es el habeas data, buen nombre y la privacidad.

1.2 Clasificación de los Datos personales

Tal y como se explicó anteriormente la naturaleza de los datos resulta ser indispensable al momento de dar un correcto tratamiento, pues no todos los datos pueden ser tratados de la misma manera. En ese sentido lo manifestó Remolina (2012), en su artículo *Aproximación Constitucional de la Protección de Datos Personales en Latinoamérica* "la protección de datos personales se amplía a cualquier naturaleza de información sobre la persona (privada, sensible, semiprivada y pública), lo cual implica que toda clase de dato personal debe ser tratado debidamente" (p.6)

En ese sentido, se han efectuado diversas clasificaciones de los datos. Sin embargo, actualmente en Colombia de acuerdo a los parámetros legales previstos en la Ley 1266 de 2008, 1581 de 2012 y los preceptos constitucionales, se ha elaborado una clasificación general, en la que encontramos los Datos públicos, privados, semiprivados, sensibles y los relacionados con los niños, niñas y adolescentes. Tal y como se explicará a continuación.

1.2.1 Datos Públicos

Los datos públicos son aquellos que no están sometido a reserva alguna y que por tanto son de conocimiento general. En ese sentido, el acceso a dicho dato no requiere autorización alguna por parte del titular.

La ley 1266 de 2008 ha definido el dato público como:

> el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas. (ley 1266,2008, art.3)

Se tiene entonces, que aquellos datos que no se encuentren dentro del listado desarrollado por la ley serán catalogados como públicos y por tanto el acceso a los mismos no tendrá ningún tipo de restricción. No obstante lo anterior, el hecho de que los datos se encuentren en plataformas digitales y que los mismos sean de fácil acceso, ello no quiere decir que en todos los casos los mismos posean una naturaleza pública.

Así lo ha explicado el Doctor Remolina:

> No debe confundirse la información pública por naturaleza jurídica con aquella que esté a disposición de público o que sea fácilmente accesible a través, por ejemplo, de internet. La información no deja de ser privada ni se convierte en pública por el mero hecho de poder consultarse fácilmente. (Remolina, 2013a, p.141)

Es claro entonces, que los datos públicos serán catalogados así, siempre que su naturaleza jurídica permita la circulación y divulgación de los mismo sin autorización previa y, por lo tanto, sean de conocimiento general sin limitaciones de ningún tipo.

1.2.2 Datos Privados

Los datos privados son aquellos que por su naturaleza jurídica gozan de una reserva y los mismos son significativos para el titular o dueño de los mismos.

Así lo definió la Ley 1266 de 2008, “es el dato que por su naturaleza intima o reservada solo es relevante para el titular” (Ley 1266,2008, art.3 literal h)

Dentro de esta categoría se encuentran datos relacionados a la información financiera, información tributaria, historias clínicas, información relacionada a patologías sujeta a reserva como el VIH, números de teléfono, correos electrónicos, entre otros.

No obstante lo anterior, si bien el dato es reservado, el acceso al mismo es posible siempre que medie autorización judicial, que se dará con ocasión al cumplimiento de sus funciones.

En ese sentido lo señaló la Corte Constitucional:

> …el legislador estatutario ha englobado las categorías de información privada y reservada. En este caso, según se ha expuesto en esta sentencia, la posibilidad de acceso a la información es excepcional, debe estar mediada de orden judicial, y se predica únicamente de aquellos datos que, siendo privados, difieren de lo que la jurisprudencia ha denominado como datos sensibles. Al respecto, debe insistirse en que el acceso a la información privada constituye una restricción apreciable de libre ejercicio del derecho a la intimidad, razón por la cual, la decisión acerca del conocimiento de la misma es un asunto que sólo puede ser decidido por las autoridades judiciales en ejercicio de sus funciones, habida consideración de la cláusula general de reserva judicial para la restricción legítima de los derechos fundamentales. (Corte Constitucional, C-748, 2011)

Se tiene entonces que los datos privados son de propiedad única y exclusiva del titular, por lo tanto, para tener acceso a los mismos debe contarse con la aprobación o la autorización del dueño de la información.

1.2.3. Datos Semiprivados

Esta categoría de datos personales si bien tienen naturaleza privada y son de interés del titular, los mismos pueden ser de conocimiento por parte de otro grupo de personas siempre y cuando medie autorización.

En ese sentido lo ha expresado la Superintendencia de Industria y Comercio en su cartilla de *Aspectos Prácticos sobre el Derecho de Habeas Data*

> Estos datos, aun cuando tienen un carácter privado solo le interesan al titular y a un grupo determinado de personas, las cuales pueden consultar la información mediando una autorización. El típico ejemplo de esta clase de datos son las historias crediticias que administran las centrales de riesgo. (SIC, 2016, p.7)

Tal y como se dijo anteriormente, uno de los ejemplos de dichos datos, son los reportes financieros, los cuales son administrados a través de las centrales de riesgo, y si bien los mismos son de propiedad del titular, dicha información puede ser de conocimiento de terceros. Ello en razón a diferentes funciones administrativas, judiciales o crediticias.

Por consiguiente, en aras de acceder a dicha información se requiere un consentimiento previo por parte del titular, consentimiento que es otorgado a las fuentes de la información a través de una autorización, documento que en el proceso de administración, recolección y consulta de la información juega un papel importante.

En ese orden de ideas, se tiene entonces que los datos semiprivados, es un rango de datos que requieren de un manejo especial, pues los mismos están condicionados y sujetos a una autorización por parte del titular. Así mismo, lo ha definido la Ley 1266 de 2008 en su artículo 3° literal g.

1.2.4. Datos Sensibles

Esta categoría de datos está directamente relacionada con la privacidad de una persona, es decir, aquellos datos que por su naturaleza revelan aspectos íntimos de cada titular. Por lo cual, los mismos gozan de una especial protección. Por lo tanto, estos datos son confidenciales.

El uso indebido de los mismos puede generar un riesgo en el respeto de garantías constitucionales como la intimidad y la libertad de una persona.

La ley 1581 de 2012 definió este grupo de datos de la siguiente manera:

> (…) se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos (Ley 1581, 2012, art. 5)

La naturaleza de dichos datos se encuentra relacionada directamente con la creación de un perfil personal, pues dentro de los datos sensibles se enmarcan aspectos como la orientación sexual, política, religiosa, entre otros Pfeiffer (2008); de ahí que la divulgación inapropiada de dicha información pueda generar perjuicios al titular de la misma.

El mal uso, circulación o administración de esta tipología de datos vulnera derechos como la honra, la dignidad o la libertad de expresión de una persona. Por tal razón gozan de especial protección por parte del Estado.

Así lo ha expresado la Corte Constitucional

> encontramos la información reservada, que por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados "datos sensibles" o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc. (Corte Constitucional, T.-729 2002)

En ese orden de ideas, para una política de tratamiento de datos personales, esta categoría de datos resulta ser importante, toda vez que el conjunto de los mismos define e identifica a una persona dentro de un espacio social o cultural en específico. En razón a ello, la difusión indebida y/o sin el consentimiento del dueño de dichos datos, fomentaría escenarios de discriminación o señalamiento, conductas negativas que afectarían directamente el buen nombre de una persona. De ahí que el tratamiento de estos datos sea “restrictivo” (Remolina, 2013b, p.151)

1.2.5 Datos relacionados con los niños, niñas y adolescentes

Si bien esta categoría de datos no hace parte de la clasificación general que se tiene de los datos personales, la misma se incluyó en la legislación colombiana con la Ley 1581 de 2012.

Es importante tener en cuenta que los niños, niñas y adolescentes son sujetos que gozan de especial protección en todo sentido, por lo tanto, en materia de datos personales no podían ser la excepción. Por lo tanto, la citada Ley reguló el tratamiento de estos datos en su artículo 7°. En éste, el legislador señaló un respeto y una prelación de los derechos de los niños, niñas y adolescentes respecto a sus datos personales.

Así mismo, obligó al estado a capacitar y a formar a los representantes y tutores de estos menores sobre el uso y circulación de los datos personales de esta población especial. Ello en aras de respetar las garantías constitucionales que poseen este grupo de personas.

Es por ello, que en el Decreto Reglamentario 1377 de 2012 se establecieron algunos parámetros y requisitos respecto al tratamiento de datos personales de los niños, niñas y adolescentes, dentro de los cuales evidenciamos: (i) interés superior de los niños, niñas y adolescentes; (ii) respeto de los derechos fundamentales; y (iii) deber de responsabilidad del encargado del uso de dichos datos.

2. Protección de Datos en Colombia

2.1. Antecedentes en Colombia sobre protección de datos personales

El derecho de Habeas Data en Colombia tiene como base regulatoria la Constitución Política de Colombia en su artículo 15, el cual predica lo siguiente:

"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. (…)" (Const.,1991, art.15)

Es así que para el Estado se crea la necesidad de velar por el respeto y la seguridad de los datos personales de los ciudadanos y lo que ello conlleva, pues es de resaltar que dicho precepto constitucional va directamente relacionado con la intimidad personal, el buen nombre y la protección especial de los datos de cada persona.

Por tal razón, el primer antecedente normativo en Colombia en materia de protección de datos nace con la expedición de la Ley Estatutaria 1266 de 2008, la cual regula aspectos específicos en materia de protección de datos.

En efecto, en dicha norma se expusieron todos los lineamientos en materia de habeas data financiero. En la misma se regularon los aspectos relacionados con la recolección y circulación de la información comercial y financiera de cada titular, la cual debía ser consignada en las bases de datos de las centrales de riesgo o también llamados operador de la información, esto con el fin de crear perfiles de crédito a través del análisis del comportamiento crediticio de cada titular.

Así lo expreso la Corte Constitucional en la sentencia C-1011 de 2008:

> La administración de datos personales sobre comportamiento crediticio es una actividad necesaria, a efectos de proteger el ahorro público y satisfacer los intereses del tráfico mercantil, actividades que prima facie no se oponen a los postulados constitucionales. Sin embargo, esta actividad está supeditada a la eficacia del derecho fundamental al hábeas data del sujeto concernido, conforme

> los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad. En consecuencia, el ejercicio de la administración de datos personales relativos al comportamiento crediticio es un ámbito de la vida social que busca fines compatibles con la Constitución. Sin embargo, esa compatibilidad no constituye una autorización ilimitada para el ejercicio arbitrario de las facultades de recolección, tratamiento y circulación de la información personal. En contrario, estas facultades sólo resultarán legítimas si (i) preservan el plexo de principios y garantías que conforman el derecho fundamental al hábeas data; y (ii) se ejercen a partir del criterio de responsabilidad social predicable de las fuentes, los operadores y los usuarios de la información. (Corte Constitucional, C-1011 de 2008).

Así mismo como componentes normativos de dicha ley se observa que se emitieron los Decretos reglamentarios 1727 de 2009 y Decreto 2952 de 2010.

En el primero de ellos, se desarrollaron todos los aspectos relacionados a la forma en la cual debía reportarse la información ante las centrales de riesgo.

Por otro lado, el Decreto 2952 de 2010, precisó los lineamientos sobre los cuales debía regularse los artículos 12 y 13 de la Ley 1266 de 2018. Artículos que regularon temas como el requisito de comunicación previa para la procedencia del reporte negativo; y el término de permanencia de la información de acuerdo a la mora en las obligaciones en los eventos de pago o ante el fenómeno de prescripción de las obligaciones. Así mismo, en este Decreto se desarrollaron aspectos relacionados al reporte negativo en aquellos casos de Fuerza Mayor o Caso Fortuito.

No obstante, lo anterior, si bien el legislador enmarco sus esfuerzos en la expedición de una norma que tratara aspectos relacionados con datos personales, la misma (Ley 1266 de 2008) no alcanzó a abarcar todos los aspectos que conlleva un tratamiento de datos personales en general. Como se dijo anteriormente, la Ley Estatutaria de Habeas Data financiero centró su objetivo en la recolección y circulación de datos comerciales y financieros para efectos de identificar riesgos crediticios. Es decir, la misma era de aplicación sectorial, pues, según

Remolina (2010), reguló en forma exhaustiva sobre el cumplimiento e incumplimiento de obligaciones dinerarias.

Sin embargo, el constante cambio y la adaptación a las nuevas tecnologías hizo que se creara nuevamente la necesidad de expedir una norma en la cual se incluyera y se regulara de manera específica todo el tratamiento y protección de los datos personales de los titulares.

En ese mismo sentido lo expresó Pérez Fernández, en su artículo *El habeas data en Colombia: su desarrollo y conexidad con los derechos fundamentales (2016):*

> Si bien es cierto la expedición de la ley 1266 representó un avance en materia regulatoria del Habeas Data, su implementación no fue la adecuada frente a todo lo que se refiere al manejo y protección de datos personales, habida cuenta que aun existían grandes vacíos que permitían que los problemas por la falta de reglamentación aumentarán; dicha problemática del manejo de las bases de datos en las diferentes entidades (públicas y/o privadas), generó la necesidad de la promulgación de una nueva ley que regulara de una manera general e integral el Habeas Data los datos personales en un ámbito diferente o lo comercial y financiero (Pérez, 2016 p.8-9).

Así las cosas, ante la necesidad de regular todo el tema relacionado con los datos personales y la protección de los mismos, se da entrada a la Ley 1581 de 2012, a través de la cual se dictan todas las disposiciones generales en materia de protección de datos personales.

Recuérdese que el sistema de protección de datos personales surge de la necesidad de controlar el uso que se le da a la información de cada persona. “En este contexto, el derecho fundamental a la protección de datos constituye el punto de equilibrio necesario que garantizará nuestros derechos y las autoridades de protección de datos están llamadas a jugar un papel esencial” (Martínez, 2007, p.60).

La promulgación de dicha norma trajo consigo un avance significativo en lo que respecta a datos personales, pues, anteriormente existían vacíos normativos notorios en esta materia que permitían generar incertidumbre e incluso una desprotección frente a un derecho tan importante.

Tal y como lo mencionó Galvis (2012) *"*la Ley Estatutaria 1581 de 2012 ha significado un adelanto importante en torno a la protección de cualquier dato personal que sea administrado por entidades públicas y privadas, de acuerdo con los principios generales establecidos en la Constitución." (p. 212).

Con la promulgación de dicha norma se logró crear una estructura detallada en materia de protección de datos, pues en esta se desarrollaron los siguientes aspectos: (i) definió de manera concreta a que personas iba dirigida la aplicación de dicha Ley; (ii) identificó y clasificó los datos objetos de protección; (iii) estableció los deberes y los derechos que poseen los titulares de la información, pues a través de estos, cada persona podía conocer de manera concreta que garantías tenía sobre sus datos y la responsabilidades que conllevaba la recolección y circulación de los mismos; (iv) estructuró en detalle una herramienta indispensable para efectos de la circulación de la información, la autorización. Así mismo como complemento reglamentario a través del Decreto reglamentario 1377 de 2013 se definió los componentes y alcances exactos de la autorización; (v) definió el procedimiento de consultas y reclamos por parte de los titulares, luego entonces, se evidenció el alcance de la norma respecto al derecho de acceso a la información, así como su rectificación, actualización o modificación. Pilares indispensables que componen el derecho de habeas data; (vi) Estructuró una política de tratamiento de datos personales, en la cuales definió roles y funciones sobre los responsables de la información y los encargados del tratamiento de la misma; y finalmente (vii) designó la autoridad de vigilancia y control en materia de datos, la cual quedo en cabeza de la Superintendencia de Industria y Comercio a través de la Delegatura de Protección de datos.

Puede evidenciarse entonces que la norma en mención abarcó todos aquellos aspectos generales en materia de datos personales. Así como también, planeó y estructuró una política de tratamiento de los mismos. Por lo cual, se atendió la necesidad de seguridad y con ello se implementó estándares y políticas de seguridad que permitieran ejerce un control adecuado en la administración de la información que fuera incluida y registrada en las diversas bases de datos.

Tal y como lo señaló Bautista en su artículo *Marco legal en Colombia, la Ley Estatutaria de Protección de Datos y el tratamiento penal* (2015)

> [Esta] Ley pretende desarrollar, de acuerdo a su objeto, un aspecto esencial del derecho al habeas data, en particular, el derecho a conocer, actualizar y rectificar información personal. Conforme a lo expresado previamente en el análisis sobre el artículo 15 constitucional, esta norma aporta su aplicación en conjunto con la garantía del artículo 20, conjugando la libertad de expresión y el derecho a la intimidad personal y familiar. (Bautista, 2015, p.7)

Así mismo, en aras de profundizar y desarrollar aspectos señalados en la Ley 1581 de 2012, se da nacimiento a la vida jurídica al Decreto 1377 de 2013, en el cual se reguló aspectos relacionados a la autorización otorgada por parte del titular para el tratamiento de sus datos personales. Se definieron las funciones y la política que debían adoptar los responsables y Encargados del tratamiento de datos personales; se definieron todas las políticas en materia de transferencia de datos, y finalmente se desarrolló los aspectos básicos y fundamentales del principio de Responsabilidad Demostrada.

Ahora bien, con el fin de controlar la recolección de datos personales por parte de todas las entidades, surgió la necesidad de implementar un Registro de Base de Datos, con el cual lo que se buscaba era identificar la cantidad, calidad y naturaleza de los datos recolectados. Ello en aras de ejercer un control sobre estos datos y la política de tratamiento a adoptar en cada caso. Fue entonces como surgió el Decreto 886 de 2014 expedido por el Ministerio de Comercio, Industria y Turismo

Es claro por tanto que el artículo 15 de la Constitución Política de Colombia fue desarrollado en su totalidad, pues con el nacimiento de estas dos normas principales, las sentencias de control Constitucional y sus Decretos Reglamentarios, no solo se ha regulado la protección de datos en materia financiera sino adicional a ello se ha regulado todo el tratamiento de datos personales.

Dentro del capítulo de anexos se adjuntan las siguientes Tablas, en las cuales se hace una breve explicación cronológica de las normas expedidas en materia de protección de datos, a saber:

a) Anexo 1.- Tabla No. 1 *Normatividad y Jurisprudencia existente en materia de Habeas Data Financiero*

b) Anexo 2.- *Normatividad y Jurisprudencia existente en materia de Protección de Datos Personales*

2.2. Principios rectores que rigen el tratamiento de datos personales a la luz de la ley 1581 de 2012

Dentro de la estructura normativa de la Ley 1581 de 2012, el legislador desarrolló ocho principios rectores, los cuales fueron expuestos en el artículo cuarto de la mencionada ley. En estos se plantearon de manera específica los lineamientos y las bases para efectuar un correcto tratamiento de datos personales. Por lo tanto, los mismos serán eje central y guía práctica para ejecutar de manera idónea una buena política de tratamiento de datos personales, pues a través de estos principios se plantean las bases de aplicación de la norma.

Así los definió el autor Remolina (2013c) "(…) aquellos postulados generales que, incluidos o no formalmente en el ordenamiento jurídico, sirven de base o de razón de ser de enunciados normativos particulares del derecho del debido tratamiento de datos personales" (p.177)

Principio de legalidad en materia de Tratamiento de datos: Este principio resulta ser el más importante en el tratamiento de datos personales, pues el mismo refiere que todo el proceso de recolección y circulación de datos debe hacerse de acuerdo a las normas vigentes para este proceso. Es decir, los datos personales no podrán ser recolectados bajo modalidades fraudulentas o con engaños.

Todo el proceso de tratamiento de datos debe encontrarse acorde a los lineamientos legales previstos para tal fin, ir en contravía de lo ya establecido haría de la recolección o el uso del dato una práctica ilícita.

La Red Iberoamericana de Protección de Datos así ha definido este principio "los datos sólo podrán ser recabados y tratados de buena fe, con estricto respeto por la Ley y los derechos de las personas y de conformidad a lo previsto en las presentes directrices" (p. 14)

Es así por tanto que dicho principio de encuentra directamente relacionado con todos los demás, pues su aplicación debe estar inmersa en todas las actividades que se tengan que desarrollar en el marco de protección de datos.

Principio de Finalidad: Este principio está ligado con el objetivo o la razón para la cual fue recolectado dicho dato. De ahí que los datos recolectados no pueden tener una destinación o uso contrario al autorizado.

La unión europea en su Reglamento General de Datos Personales en su artículo 5° así ha definido este principio "Los datos personales será recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (…)" (RGDP, art.5)

Luego entonces aquellos usuarios que recolecten datos personales deben tener en claro que el uso de los mismos debe tener un fin específico, ir en contravía de ello, demostraría una conducta ilegal, pues se sobrepasan los límites autorizados para su destinación. "Esto significa que no podrán solicitarse ni registrarse más datos que los estrictamente necesarios para llevar a cabo la finalidad de que se trate, aunque fuesen susceptibles de serlo para cumplir objetivos futuros" (Observatorio Iberoamericano de Protección de Datos, 2013)

Por lo tanto, este principio lo que "busca es evitar que se recolecten datos para hacer con ellos lo que sea y delimita los usos que el responsable, encargado o usuarios pueden dar a la información en comento" (Remolina, 2013d, p.182)

Principio de Libertad: Este principio va directamente relacionado con el consentimiento del titular o dueño de la información. Tal y como se expone en el artículo 4° literal c) "El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento" (Ley 1581, 2012)

Se tiene entonces que el principio de libertad en relación con la protección al derecho a la intimidad está directamente ligado a que "los datos personales de un individuo solo pueden ser revelados con su consentimiento expreso o tácito…" (Bautista, 2015, p. 31)

Es por ello, que el consentimiento del titular debe verse expreso en una autorización, documento que para efectos del tratamiento de datos personales juega un papel importante, pues a través de este, el titular otorga su permiso para que sus datos personales sean destinados para una labor en específico. Con ello lo que se busca es "legitimar el tratamiento de datos personales" (Remolina, 2013e, p.191)

Por lo tanto, el consentimiento del titular debe ser libre de tal manera que éste pueda tener claridad sobre el uso y tratamiento que va a recibir sus datos.

Así lo expresó el Parlamento Europeo en su reglamento:

> El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. (Reglamento Europeo, Considerando 32)

Vale la pena aclarar entonces que la autorización debe ser expresa, clara y en la misma debe delimitarse la finalidad y la temporalidad del tratamiento de dichos datos.

Principio de Veracidad o Calidad: Este principio está directamente relacionado con la realidad y actualidad del titular. Es decir que la información debe ser real, exacta y actualizada. La imparcialidad de dicha información viola notoriamente el derecho de habeas data y buen nombre de los titulares, pues claramente todos aquellos datos incorrectos, incoherentes, o desactualizados pueden arrojar información que no corresponde al titular. "Los datos deberán mantenerse exactos, completos y puestos al día, respondiendo a la verdadera situación de la persona a la que se refieran" (Viega, 2010, p. 4)

Principio de trasparencia: El artículo 4° de la Ley 1581 de 2012 literal e, señala que: "En el Tratamiento debe garantizarse el derecho del titular a obtener del responsable del

tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan" (Ley 1581, 2012, art. 4)

Se tiene entonces que la definición de este principio va directamente relacionada con el derecho que tiene todo titular de conocer sus datos personales. Quiere ello decir entonces que la persona tendrá acceso a toda la información relacionada con el tratamiento y la política de protección que actualmente se desarrolla y de la cual están siendo beneficiados sus datos personales. Se debe entonces, como lo menciona Rojas (2014) "garantizar al titular, cuando lo requiera y sin restricciones, el derecho a obtener información acerca de la existencia de datos que le conciernan por parte del responsable del tratamiento de sus datos".

En ese sentido, en aras de dar aplicación y materializar el principio de transparencia, la Corte Constitucional señaló que el principio de transparencia debe entonces "permitir a cualquier ciudadano establecer con exactitud quiénes son los responsables y encargados del tratamiento de sus datos (…)" (Corte Constitucional, C-748, 2011).

Principio de acceso y circulación restringida: Este principio se encuentra incorporado en el artículo 4 de la ley 1581 de 20112 literal f), el cual señala lo siguiente:

> "El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;
>
> Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley" (Ley 1581, 2012, art. 4°)

En ese orden de ideas, se observa que el legislador limitó el acceso y la circulación de dichos datos a todas aquellas personas autorizadas para tal fin.

En efecto, el presente principio, busca generar controles de seguridad en lo que respecta al acceso de los datos. No sobra poner de presente, que estos datos no serán de naturaleza pública.

En ese orden de ideas quienes efectúen el tratamiento de datos personales tendrán que tener ciertas restricciones para ello, el acceso y tratamiento solo estará en cabeza de aquellos que se encuentren autorizados para tal fin (responsables - encargados). De lo contrario, no es correcto que se tenga acceso a los datos de manera deliberada.

Por otro lado, respecto a la circulación de dicha información, la misma también tendrá que verse limitada. Es decir que el envío o transferencia de dichos datos, también será condicionada. No puede entonces convertirse en una red de tráfico de datos sin ejercer los respectivos controles y restricciones de seguridad.

Por lo tanto, los datos serán suministrados única y exclusivamente a las personas autorizadas para ello, que, para el caso en particular, las mismas se encuentran definidas en la Ley 1581 de 2012 en su artículo 13. Luego entonces, suministrar datos personales de manera irresponsable a personas no autorizadas pone en riesgo la privacidad y la integridad de la persona.

Principio de Seguridad: Tal y como se ha explicado durante el trascurso del presente escrito, los datos personales son un activo de suma importancia. Luego entonces, el cúmulo de datos personales suministran información relevante que hacen parte de la órbita de la privacidad y la intimidad de una persona.

En razón a ello y a la magnitud de información que los datos personales proporcionan, los mismos deben gozar de una protección especial en lo que respecta a su circulación, administración, manipulación y en general en lo que respecta al tratamiento de estos. Por lo tanto, los estándares de seguridad deben ser altísimos, y las políticas desarrolladas en materia de protección deben por tanto garantizar la calidad de la información.

Por lo tanto, este principio busca que se adopten las medidas de seguridad necesarias y efectivas en el proceso de tratamiento de datos personales. Ello en aras de mitigar el riesgo en

eventos como perdidas de información, adulteración de la misma, desactualización en la información administrada, entre otros. Riesgos que podrían poner en peligro la calidad de la información.

Por lo tanto, es deber de los sujetos intervinientes, controlar que la información administrada goce de total seguridad, para lo cual tendrán que implementar técnicas especializadas en seguridad informática, planes de contingencia, planes de identificación de riesgos y en general adoptar todas las estrategias posibles con las cuales se permita adoptar un plan completo de seguridad que permita tener total confiabilidad sobre los datos recolectados en el proceso de tratamiento de datos

Principio de Confidencialidad: Lo que busca este principio es conservar la discreción en la difusión de dicha información.

Por lo tanto, aquellas personas que intervienen en el proceso de tratamiento de datos personales están en la obligación de guardar total confidencialidad en el suministro de la información manejada. Quiere ello decir, que las personas intervinientes, no podrán revelar o suministrar la información que es o ha sido de su conocimiento con ocasión a su actividad o a su gestión dentro del proceso de tratamiento.

Así lo manifestó la Agencia Española de Protección de Datos en su artículo *Estándares Internacionales sobre Protección de Datos Personales y Privacidad - Resolución de Madrid*:

> "La persona responsable y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal deberán respetar la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el interesado o, en su caso, con la persona responsable" (Agencia Española de Protección de Datos, 2009)

Luego entonces, lo que se pretende con la adopción de dicho principio, es evitar poner en riesgo la información. Claramente el principio de confidencialidad se encuentra directamente relacionado con el secreto profesional, pues quien ejerce una labor dentro del tratamiento de

datos personales, no podrá divulgar la información que ha conocido con ocasión al ejercicio de sus funciones.

2.3. La Autorización como medio de recolección y circulación de Datos Personales

La autorización resulta ser un aspecto de suma importancia en todo lo que respecta al tratamiento de datos personales, pues la misma va ligada directamente con el consentimiento del titular de la información. De ahí que ésta sea el eje central de todo este proceso. De no existir el consentimiento previo por parte del titular, los responsables o encargados del tratamiento de los datos no podrían recolectar ni mucho menos circular datos. Luego entonces, no se tendría potestad de uso sobre dicha información.

Este requisito, fue incluido en la Ley 1581 de 2012 en su artículo 9°, en el cual se precisó la necesidad y exigencia de la autorización para el trato de datos personales. A su vez, éste fue desarrollado de manera específica en el Decreto 1377 de 2013 (artículos 4-12). En este, se definieron todos los aspectos relacionados con el contenido de la autorización, la finalidad y limitación de la misma y los lineamientos respecto a la recolección, uso y circulación de los datos sensibles y de los datos de los niños, niñas y adolescentes.

Ahora bien, la ley 1581 de 2012 ha definido la autorización como el "Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales" (Ley 1581, 2012, art. 3°).

Se tiene entonces que el legislador le ha dado esa potestad al titular de decidir sobre el tratamiento de sus datos. Por tal razón, la inexistencia de dicho consentimiento podría plantear dos posibles escenarios; por un lado, la negativa por parte del titular de suministrar sus datos o por el contrario, una ilegalidad en la recolección y uso de los mismos. Es por esta razón, que la exigencia de la autorización resulta ser indispensable y sin ecuánime.

Adicional a ello, en aras de garantizar el precepto constitucional consagrado en el artículo 15 de la Constitución Política, se hace necesario que cada titular pueda disponer de sus datos. Así como también conocer el manejo que estos tengan.

Ahora bien, dentro de la definición de *Autorización*, se identificaron varios conceptos, los cuales, coinciden en asegurar que ésta es un medio a través del cual se obtiene el consentimiento del interesado, a través de su manifestación libre y voluntaria acerca del tratamiento de sus datos personales.

En efecto, la Superintendencia de Industria Comercio en la Cartilla de formatos modelo para el cumplimiento de obligaciones establecidas en la ley 1581 de 2012 y sus decretos reglamentarios, definió la autorización como "El consentimiento que da cualquier persona para que las empresas o personas responsables del tratamiento de la información, puedan utilizar sus datos personales." (SIC, 2017, p. 7)

La autorización debe contener tres características importantes. Ésta debe ser libre, previa y expresa.

Debe ser libre, pues, es un consentimiento propiamente del titular y por ende su otorgamiento debe ser de manera voluntario, no debe existir una condición obligatoria. Tampoco debe coaccionarse al titular para el suministro de la misma.

Debe ser previa, pues, antes de concederla, el titular debe conocer que uso tendrán sus datos. De concederse la autorización de manera posterior, la finalidad de dicho requisito desaparecería.

Por otro lado, debe ser expresa, pues los aspectos que se consignen en la misma, deben ser claros, de tal manera que el dueño de la información conozca para que fin fueron recolectados sus datos y la destinación de los mismos.

Así lo ha señalado Corte Constitucional:

> Debe ser expresa y voluntaria por parte del interesado, para que sea realmente eficaz, pues de lo contrario no podría hablarse de que el titular de la información hizo uso efectivo de su derecho. Esto significa que las cláusulas que en este sentido están siendo usadas por las distintas entidades, deben tener una forma y un

> contenido que le permitan al interesado saber cuáles son las consecuencias de su aceptación. (Corte Constitucional, SU 082, 1995)

Téngase en cuenta además que el consentimiento del titular debe ser contundente, no es permitido aceptaciones implícitas.

Nótese entonces que una vez más los principios rectores son la base del tratamiento de datos personales, pues la autorización no solo es un requisito que va de la mano del principio de libertad, sino adicional a ello, va ligada también al cumplimiento del principio de finalidad.

Ahora bien, la autorización podrá ser otorgada de manera escrita, oral, o mediante una figura llamada las Conductas inequívocas del titular de la información. No obstante, en cualquiera de los tres casos la entidad o persona encargada de efectuar el tratamiento de los datos, está en la obligación de guardar prueba de la misma, pues así lo ordenó la Ley.

Respecto a las conductas inequívocas del titular de la información, es importante resaltar que a través de este medio, la ley quiso regular ciertos eventos o actuaciones que si bien no pueden tomarse como un consentimiento expreso, el trasfondo de dicha actuación permite identificar una aceptación en el tratamiento de los datos. Así lo estableció el Decreto 1377 en su artículo 7° "mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización…" (Decreto 1377, 2013, art. 7). En estos casos, debe existir una conducta por parte del titular con la cual da a entender su deseo de que sus datos sean tratados.

En ese orden de ideas, es claro entonces que, si bien el titular no suscribió una autorización de manera expresa, su actuar indirectamente reflejó una aceptación; este fenómeno puede asemejarse con una conducta concluyente.

Para esto es importante que, "la conducta del titular [indique] claramente que acepta el tratamiento de su información." (Remolina, 2013f, p. 194). El ejemplo más típico con el que se puede ilustrar este medio, es el aviso que se le da a las personas cuando su imagen está siendo tomada por cámaras de seguridad.

En todo caso, este medio de autorización genera un riesgo respecto del consentimiento del titular, pues muchas de las actuaciones inequívocas no pueden ser interpretadas como una aceptación. Adicional a ello, dada la generalidad de dicha autorización y lo poco especifica que puede llegar a ser, nos encontraríamos frente a una duda respecto de los alcances y los límites de la misma. Es de decir, ¿hasta qué punto pueden ser tratados esos datos? Luego entonces, existen vacíos normativos frente a este tipo de autorización que valdría la pena que el legislador profundizara.

Ahora bien, si bien durante el presente capítulo se ha insisto en la necesidad de la exigencia y el otorgamiento de la autorización, en cualquier caso, el legislador ha previsto unas excepciones dentro de las cuales no será obligatorio la solicitud de una autorización, las mismas se encuentran enmarcadas en el artículo 10 de la Ley 1581 de 2012.

Es así que la autorización en materia de protección de datos, resulta ser un requisito indispensable para el tratamiento de los datos, un mínimo error en la elaboración y contenido de la misma, o por el contrario en la omisión en el cumplimiento de éste, puede acarrear una vulneración en el derecho a la privacidad del titular o un riesgo inminente frente al derecho de la autodeterminación.

Téngase en cuenta que el derecho a la autodeterminación, es aquel que le permite al titular, ejercer un control sobre su información personal. Además de "[establecer] un límite que determine la legitimidad del acopio, procesamiento y transmisión de [la] información, de forma que tales operaciones compatibilicen los derechos fundamentales de las personas (…)" (Cerda, 2003, p.51). Por lo tanto, a través de la autorización, puede adoptarse controles respecto de la recolección de datos, así como también la circulación de los mismos, pues es el fin último de esta, es proporcionar al titular un conocimiento y a la vez una seguridad acerca del uso y destinación que tendrán sus datos personales.

3. Tratamiento de Datos Personales

3.1. Principio de Responsabilidad Demostrada (accountability) como mecanismo efectivo para el tratamiento de datos personales

Este principio tiene como objetivo velar por el respeto y la privacidad de los datos personales. Es decir, que lo que se busca con este principio es que se desarrollen políticas y procedimientos que garanticen un adecuado tratamiento de datos, de tal manera que, a través de estos, se pueda demostrar una correcta gestión en la recolección, administración, uso y circulación de los datos registrados en las diferentes bases de datos.

Así se estableció en el Decreto Reglamentario 1377 de 2013 en su artículo 26

> 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 (…) (Decreto 1377, 2013, art. 26)

Es por eso, que aquellas entidades o personas encargadas de la recolección de datos personales, deben desarrollar políticas de seguridad de acuerdo a los lineamientos legales expuestos para ello, pues a través de las mismas se garantiza el respeto a los principios establecidos en materia de protección de datos.

Dichas políticas deben estar orientadas en implementar y certificar cada uno de los procedimientos que se llevan a cabo en pro de efectuar un buen tratamiento de datos personales. Ello, con el fin de vigilar que cada operación en materia de protección de datos no se vea expuesta a riesgos.

De ahí que el principio de Responsabilidad Demostrada se encuentre relacionado con el principio de seguridad, pues en este caso, los responsables y encargados de dicho tratamiento deben adoptar estratégicas que estén encaminadas en asegurar cada dato que se recolectó y que este siendo objeto de tratamiento. Vale la pena resaltar que estas medidas a adoptar deben ser herramientas humanas, tecnológicas, organizacionales, administrativas, legales, entre otras.

Así se enfatizó en la *Guía GECTI para la implementación del principio de responsabilidad demostrada —accountability— en las transferencias internacionales de datos personales:*

> Dicho principio exige que los responsables y encargados del tratamiento de datos, implementen medidas apropiadas, efectivas y verificables que les permitan probar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, el Programa Integral de Gestión de Datos Personales (PIGDP) se constituye en un mecanismo operativo para realizar todo lo necesario con miras a garantizar el debido tratamiento de los datos personales. (Remolina Angarita y Álvarez Zuluaga 2018)

En ese mismo sentido lo ratificó la Superintendencia de Industria y comercio como ente encargado de vigilar la correcta administración de datos personales, en la *Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability)*:

> Estas políticas internas efectivas no pueden limitarse a reproducir los textos legales ni son meras declaraciones de principios. Por el contrario, la adopción de políticas internas efectivas parte del Desarrollo de un Programa Integral de Gestión de Datos Personales, que debe ser el resultado de un proceso de debida diligencia al interior de la organización que permita formularlo. (Superintendencia de Industria y Comercio, 2015, p. 9).

Por lo tanto, para el desarrollo de dicho principio resulta menester hacer una revisión al detalle de aspectos como: la cantidad de bases de datos manejadas, la calidad y la clase de datos que están siendo recolectados en las mismas, la finalidad de dichos datos, los estándares de seguridad que actualmente se manejan respecto a la circulación de los mismos y en general efectuar una revisión de cómo se encuentra la Compañía en tratamiento de datos para así, determinar qué aspectos se están desarrollando acorde a la normatividad vigente y por otro, identificar las debilidades. De esta manera se logra tener un diagnóstico de que tanto la Compañía cumple con las políticas de seguridad.

Ejemplo de la aplicación de dicho principio, lo encontramos en el diagnostico efectuado por parte de Fernández Pedrosa (2017), a través de su práctica empresarial *Guía de*

Implementación y lecciones aprendidas para el proyecto de aplicación de la ley de protección de datos personales –Fiduprevisora-, pues en aras de elaborar un buen sistema de protección de datos, guardando congruencia con el principio de Responsabilidad Demostrada, el autor efectúo un análisis en detalle del estado interno y externo de la Compañía en materia de protección de datos. Identificó los factores de éxito y los factores críticos de la Compañía y analizó el sistema vigente para dicha época en materia de protección de datos. Todo ello, con el fin de implementar las correcciones necesarias a través de un nuevo sistema metodológico que garantizara un correcto tratamiento de protección de datos, ajustado a los lineamientos legales para ello. Luego entonces, efectúo una correcta aplicación del Principio de Responsabilidad Demostrada.

Recuérdese entonces que el principio de responsabilidad demostrada

> (…) exige que las organizaciones establezcan políticas internas, que sean efectivas, en orden a garantizar diferentes aspectos entre los que cabe señalar, los que se citan a continuación: (i) que la organización exista una estructura administrativa proporcional a la estructura del responsable para implementarlas; (ii) que se adopte mecanismos internos para poner en práctica las políticas que incluyan herramientas de implementación, entrenamiento y programas de educación y formación que abarque el conjunto de la organización; y (iii) la adopción de procesos para la atención de reclamaciones y cualquier consulta que puede llevar a cabo los titulares de los datos, que sean objeto de tratamiento (Puyol, 2017).

Ahora bien, la implementación o la adopción del principio de Responsabilidad Demostrada, resulta ser un aspecto práctico, en el cual debe trabajarse constantemente, pues con los avances tecnológicos, tanto el suministro de datos como el tratamiento de los mismos, debe estar en constante actualización, de tal manera que los estándares de seguridad se vean cada vez más reforzados y con ello se mitigue los posibles riesgos. Para lo cual, es necesario que se efectúe una evaluación general, a través de la cual se van a identificar aspectos medulares que permitirán de esta manera adoptar correctivos y medidas que garanticen un buen tratamiento de datos. El artículo 26 del Decreto 1377 de 2013, enumeró ciertos aspectos que deben ser tenidos en cuenta:

(i) La naturaleza jurídica del responsable – tamaño empresarial: Este aspecto permitirá identificar qué tipo de naturaleza es la empresa y su estructura organizacional (grande, mediana o pequeña). Ello permitirá dimensionar el flujo de datos manejado y circulado al interior de la Compañía

(ii) La naturaleza de los datos: la calidad de los datos recolectados objeto de tratamiento, permite determinar el tratamiento en específico que debe dársele.

(iii) El tipo de tratamiento: este aspecto obedece a la metodología a usar. Es decir, el tratamiento podrá hacerse de manera automática o manual. Con esto lo que se busca es evaluar la efectividad y la garantía que emite cada herramienta usada.

(iv) Los riesgos que se puedan presentar en el tratamiento de datos: Este aspecto, lo que busca es identificar los riesgos en materia de protección de datos. Así como también calificar los mismos. De esta manera, lo que se busca es adoptar planes de contingencia que permitan controlar y suprimir dichos riesgos.

Es así como a través del Principio de Responsabilidad demostrada, lo que se busca es que el proceso de tratamiento de datos se encuentre acorde a los lineamientos legales y que de esta manera, se pueda garantizar una correcta administración de datos a través del cumplimiento y adopción de todos los parámetros existentes en esta materia. Así lo expresó Quiroga (2014) en su artículo *Aplicación del Principio de Responsabilidad Demostrada:*

> De este modo, con la aplicación del principio de la responsabilidad demostrada, se crean mecanismos estables y seguros para los ciudadanos respecto al tratamiento efectivo de sus datos personales, es decir que estos sean tratados para los fines concretamente autorizados y con los más altos estándares de protección y confidencialidad. (Quiroga, 2014)

Recuérdese que los datos personales, son activos que merecen una especial protección y, por lo tanto, su tratamiento debe respetar garantías de seguridad, confidencialidad y calidad.

3.2. Sujetos que intervienen en el Tratamiento de Datos Personales

La ley 1581 de 2012, destacó la participación de tres sujetos en el proceso de tratamiento de datos personales, Los Titulares, Los Responsables y los Encargados.

Los sujetos anteriormente mencionados, son los Sujetos que intervienen de manera activa en todo el proceso de tratamiento de datos personales. Sobre ellos radica la responsabilidad de que dicho tratamiento se efectúe de manera correcta, cumpliendo los lineamientos legales para tal fin en aras de cumplir y atender en debida forma al principio de Responsabilidad Demostrada.

Respecto al Titular de los datos personales, debe entenderse este como la persona dueña de su información, En ese mismo sentido, la ley lo definió como "la persona natural cuyos datos personales sean objeto de tratamiento" (Ley, 1581, 2012, art. 3)

Luego entonces, dentro de dicha relación, este sujeto interviniente es aquel sobre el cual versa la protección de sus derechos fundamentales y, por lo tanto, cada política de tratamiento y estrategia que se quiera implementar, estará encaminada a velar por la protección y la seguridad de los datos recolectados de este.

Ahora bien, como dueño de sus datos personales, el titular tendrá total potestad sobre sus datos. Luego entonces todos aquellos que participen en este acopio, recolección y administración deberán garantizarle a éste, la posibilidad de acceder a sus datos y ejercer los derechos o acciones que correspondan en aras de velar por su protección.

Así mismo, con el fin de que la información corresponda a su realidad, el titular tendrá el derecho de solicitar la actualización, rectificación y supresión de dicha información. Así lo estableció el artículo 21 de la Ley 1581 de 2012. Para lo cual, este deberá acatar las medidas correspondientes que se hayan destinado para tal procedimiento.

Luego entonces, es claro que el titular de la información según Ruiz (2016) podrá:

> Aclarar o agregar la información que se encuentre en un banco de datos para que el registro sea verdadero y completo, lo que se traduce en que constantemente deba ser actualizado por parte del responsable de su tratamiento y permita obtener un perfil correcto del titular de la información, evitando incurrir en errores acerca de la realidad actual y consecuentemente pueda llegar a generarle un perjuicio (Ruiz, 2016 P. 22).

Así mismo, como se ha insistido, el titular de los datos, tendrá la facultad de decidir sobre el suministro, recolección y circulación de sus datos. Es por ello, que a través de la autorización, podrá permitir el uso y la finalidad de los mismos. Por lo tanto, en cualquier instante podrá solicitar copia y prueba de dicha autorización, pues a través de la misma podrá verificar una legitimidad en la recolección de sus datos, el uso de los mismos, la limitación en cuanto a la circulación de ellos y adicional ello, definir el acceso de sus datos.

Se tiene entonces, que como propietario de sus datos, tendrá total facultad de disposición sobre los mimos como garantía y respeto a su derecho de habeas data.

Respecto al Responsable, la Ley 1581 de 2012 lo definió como la "persona natural o jurídica, pública o privada que por sí misma o en asocio con otros, decida sobre las bases de datos y/o el tratamiento de los datos" (Ley 1581, 2012, art 3.)

Luego entonces, se tiene que este sujeto tiene una participación relevante dentro del proceso de tratamiento de datos personales, pues, será quien recolecte y de uso y destinación a dichos datos. Resulta menester señalar que, la recolección y el uso de los mismos, tendrá que hacerse bajo el cumplimiento estricto de los estándares y políticas de tratamiento destinadas para ello.

En este punto, se observa entonces que el Responsable es quien debe velar porque el Principio de Responsabilidad Demostrada se cumpla, pues será quien idee cada una de las estrategias y las metodologías en materia de seguridad y riesgos.

En ese sentido lo señaló la Comisión Europea a través de su *Grupo de Trabajo de Protección de Datos del artículo 29*, al indicar que el responsable tendrá la obligación de

> "(…) aplicar medidas reales y eficaces de protección de datos orientadas a la buena gobernanza de protección de datos y que, al tiempo, minimicen los riesgos jurídicos, económicos y de prestigio que podrían derivarse de una práctica precaria de protección de datos." (Comisión Europea, 2010, p.5)

Dentro de sus deberes, tenemos que inicialmente le asiste un deber principal con el titular de la información, pues debe velar porque se cumplan todos los requisitos necesarios e indispensables en el proceso de recolección, administración y circulación de sus datos. Por lo

tanto, tendrá que verificar requisitos como el cumplimiento de la autorización, que la misma cumpla con las exigencias legales previstas.

Quizás uno de los deberes más importantes del Responsable del tratamiento de datos según Becerra, Sanchez, Torres, García y C.B & Cotino, (2015), es el de "garantizar que la información que posee en sus bases de datos sea veraz, completa, exacta, actualizada, comprobable y comprensible, ya que este es el núcleo central del derecho de *habeas data.*" (p.168)

Por otro lado, tendrá que insistir en el cumplimiento de principios como el de finalidad y seguridad de la información. Así mismo, debe centrar su actuar en una correcta manera de administrar y tramitar las consultas y requerimientos de los titulares de la información, pues tal y como se explicaba anteriormente, es importante que el canal de comunicación entre titular y responsable sea efectiva y oportuna.

Por consiguiente, su participación dentro del proceso de tratamiento de datos personales, juega un papel indispensable, pues a través de él se deben guiar todos los lineamientos en dicha materia; "es quien determina los fines y los medios del tratamiento de datos personales" (Becerra et al, 2015, p.160)

Finalmente, en lo que respecta al Encargado, la ley lo definió como aquella "Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos." (Ley, 1581, 2012, art. 3)

Por lo tanto, el encargado del tratamiento de los datos personales actuará bajo los lineamientos dados por parte del Responsable.

Tal y como lo menciona Remolina, "Realizar cualquier operación de tratamiento en nombre del responsable es lo que determina que una persona u organización sea catalogada como encargado" (Remolina, 2013g, p. 117)

En todo caso, si bien el encargado actúa a través del responsable, ello no implica que el cumplimiento de sus funciones sea independiente, al contrario de ello, estos dos sujetos tienen una responsabilidad compartida o solidaria. Por lo tanto, ante un eventual incumplimiento o desempeño erróneo en el tratamiento de datos personales, tanto el responsable como el

encargado del tratamiento de datos personales tendrán que responder de manera solidaria. Así lo estableció la Corte Constitucional en sentencia C-748 de 2011. De ahí la importancia que tiene el cumplimiento de cada una de las obligaciones.

En ese orden de ideas, es deber del encargado del tratamiento de los datos personales, al igual que el responsable, garantizar al titular la protección de su información. Por lo tanto, este sujeto, también debe implementar políticas de seguridad efectiva y ejercer los controles necesarios para que la recolección y tratamiento de datos personales se haga en debida forma.

En general, debe responder por la calidad de la información objeto de tratamiento, por lo tanto, debe velar porque se cumpla a cabalidad cada uno de los requisitos necesarios para ejercer un correcto tratamiento de datos personales. Lo anterior, con el objetivo de respetar todas las garantías relacionadas con la seguridad y la confidencialidad de la información.

3.3. Políticas efectivas en el tratamiento de la información bajo los lineamientos de la Ley 1581 de 2012

En Colombia con la expedición de la Ley 1581 de 2012 y con su Decreto Reglamentario 1377 de 2012, se desarrollaron y ampliaron todos los parámetros que debían ser tenidos en cuenta respecto a las políticas de tratamiento de la información que debían realizar todos aquellos Responsables y que a su vez las mismas debían ser acatadas por los Encargados del tratamiento de datos personales.

En ese sentido el artículo 13 del Decreto Reglamentario 1377 de 2013, definió los parámetros bajo los cuales dichas políticas debían ser elaboradas.

Así las cosas, en razón a la labor que cada uno de los sujetos desempeña dentro del tratamiento de datos personales y en aras de adoptar una buena Política de Tratamiento de Información, responsables y encargados deben elaborar un Manual Interno de Políticas, en el cual se consignarán todas las reglas y parámetros que definirán su labor.

Así lo señaló la Superintendencia de Industria y Comercio en su cartilla de Formato de Datos Personales:

> Los responsables y encargados del tratamiento de datos personales tienen la obligación de tener un manual interno de políticas y procedimientos en el que se expliquen claramente todos los parámetros y reglas que utilizará la organización para garantizar el correcto tratamiento de los datos personales, en especial, el procedimiento que la organización utilizará para atender las quejas, consultas y reclamos presentados por los titulares en ejercicio de su derecho de habeas data. (SIC, 2017, p.10)

Se tiene entonces que el manual interno de políticas es un documento diferente a las Políticas de Tratamiento de la Información. Éste guarda estrecha relación con el principio de transparencia, pues a través de estas lo que se busca es informar al titular sobre el tratamiento al cual estarán sometidos sus datos personales y la finalidad de los mismos; lo que garantizara a éste la protección de su información.

Ahora bien, resulta pertinente señalar, que actualmente el Manual Interno de Políticas debe contener información relacionada con:

(i) Los procedimientos a usar para la recolección o recopilación de la información
(ii) Las reglas respecto a la recolección, uso circulación y supresión de la información
(iii) Requisitos bajo los cuales debe ser obtenida la autorización por cada uno de los sujetos
(iv) Acceso y corrección de los datos
(v) Conservación y eliminación de la información
(vi) El uso responsable de la información, incluyendo los controles de seguridad previstos para ello. Es decir, usuarios, claves, aplicativos etc.
(vii) Todos los aspectos relacionados a las cláusulas de confidencialidad
(viii) Procedimiento interno del manejo de las consultas, quejas y reclamos

Por consiguiente, a través de estos manuales internos se regula en específico las operaciones a nivel interno de las organizaciones.

Ahora bien, respecto a las Políticas de Tratamiento de la Información, lo que se busca con la elaboración de las mismas

> Es informar y definir tanto las reglas de tratamiento de datos personales en una organización como las pautas para que el titular ejerza sus derechos. Se quiere que el titular, por ejemplo, en cualquier momento conozca los datos de contacto del responsable o encargado, los usos que se darán a la información sus derechos y la forma de ejercerlos. (Remolina, 2013 h, p. 98)

Por lo tanto, atendiendo al principio de transparencia, lo que se busca es que todas las herramientas, metodologías, medidas de seguridad y procedimientos que se vayan a usar en el tratamiento de datos personales, sean de conocimiento por parte de los titulares y de esta manera se garantice un correcto tratamiento.

Dentro de la estructura de dichas políticas de tratamiento de la información, se tiene que las mismas deben contener todos los aspectos que enumera el Artículo 13 del Decreto 1377 de 2013: (i) Aspectos que obedecen a la identificación de la persona o entidad que será el Responsable; (ii) el tratamiento al cual serán sometidos los datos recolectados; (iii) los derechos que le asisten al titular; (iv) la persona encargada de atender las peticiones consultas o reclamos de los titulares; y (v) el procedimiento para la actualización rectificación o supresión de información.

Se observa entonces, que en estas se incluye de manera expresa, todo el tratamiento que se le darán a los datos personales del titular. Por lo tanto, si bien estas serán plasmadas a través de un documento, las mismas deben tener aplicabilidad expresa. Dicha política debe ser observada y puesta en práctica por el personal que se encuentre desempeñando las labores de responsable o encargado dentro de una Compañía.

Ahora bien, la Política de Tratamiento de la Información debe ser de conocimiento de los titulares. Por lo tanto, la misma debe ser publicada a través del medio que cada organización considere efectivo, haciendo uso de las diferentes herramientas tecnológicas o las que a potestad considere necesarias, siempre y cuando la misma cumpla su deber de publicidad.

Sin embargo, puede presentarse escenarios en los cuales dicha política no pueda ser circulada y por lo tanto el Titular no pueda conocer de la misma. En estos casos, en Colombia, la ley junto con su decreto reglamentario incluyó una opción de comunicación a través de la figura del Aviso de Privacidad.

Entiéndase este como

> una de las opciones de comunicación verbal o escrita que brinda la ley para darle a conocer a los titulares de la información, la existencia y las formas de acceder a las políticas de tratamiento de la información y el objetivo de su recolección y uso. (SIC, 2017, p.11)

Por lo tanto, a través de este mecanismo lo que se busca es agotar todas las formas posibles de comunicación hacia el titular respecto del tratamiento de sus datos y la política adoptada, con lo cual se evita que el titular desconozca este tipo de información. Así se configuró en el Decreto 1377 de 2013 en su artículo 14. Este medio de comunicación solo se debe agotar sino es posible que el titular conozca la política de tratamiento de la información adoptada por cada entidad o persona. Luego entonces el mismo es un mecanismo subsidiario de la política de tratamiento de información.

El medio de difusión del aviso de privacidad podrá hacerse a través de cualquier medio, escrito, electrónico, verbal o cualquier medio que el responsable considere efectivo.

Ahora bien, respecto al procedimiento para el adecuado tratamiento de datos personales, se tiene que el responsable o el encargado del tratamiento de datos debe diseñar e implementar un procedimiento para efecto de atender solicitudes relacionadas con el acceso, la actualización, supresión, rectificación de datos y la revocatoria de la autorización. Información que deberá quedar consignada dentro de la Política de Tratamiento de la Información. Ello en aras de garantizar el acceso a la información que tiene el titular, así como también el derecho que tiene a presentar reclamaciones respecto de sus datos.

Por otro lado, resulta menester precisar que, dentro de la política de tratamiento de la información, debe designarse una persona o un área que asuma la protección de datos personales

y a su vez que asuma el trámite de las solicitudes de los titulares tal y como lo establece el artículo 23 del Decreto reglamentario mencionado en el transcurso de presente escrito. En algunos casos, estos son llamados oficiales de privacidad o Delegados de Protección de Datos.

Si bien en Colombia no se encuentra definido las características y el rol que debe desempeñar este sujeto dentro del Tratamiento de Datos personales, ya que la inclusión de esta figura es reciente en nuestra legislación, se tiene que el mismo debe desempeñar una función de dirección frente a las solicitudes propuestas por los titulares. A su vez, es pertinente aclarar que no en todos los casos es de obligatorio cumplimiento la designación de dicho cargo, pues se presentan diversos factores de tipo organizacional que pueden influir en esto.

Para la Superintendencia de Industria y Comercio la función del oficial de protección de datos

> es la de velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta para cumplir las normas, así como la implementación de las buenas prácticas de gestión de datos personales dentro de la empresa. El oficial de privacidad tendrá la labor de estructurar, diseñar, y administrar el programa que permita a la organización cumplir las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente. (SIC, 2015, p.10)

Por consiguiente, la figura del oficial de protección de Datos podrá ser adoptada por las entidades, para efectos de garantizar un adecuado tratamiento de datos, pues a través de la dirección que ejerza este personaje, se puede tener garantía y confiabilidad en el tratamiento de los datos.

Una vez recopilado todos los aspectos relacionados con la política de tratamiento de información que actualmente se desarrolla en Colombia a través de la Ley 1581 de 2012 y su Decreto reglamentario 1377 de 2013, se observa que el universo de los datos personales tiene una gran extensión y que la protección de los mismos va ligada a desarrollar un Sistema de Gestión de Datos Personales, en el cual se desarrollen un conjunto de políticas y procedimientos

con los respectivos controles de seguridad con los cuales se busca proteger los datos personales que los titulares suministran a los responsables o encargados de dicho tratamiento.

Así las cosas, lo que se busca entonces con la actual legislación es que las organizaciones y en general las personas encargadas de efectuar tratamiento de datos personales desarrollen programas efectivos de gestión de datos personales en los cuales se dé estricto cumplimiento a los lineamientos legales establecidos para ello.

En efecto, de la revisión realizada se observa que Colombia actualmente ha desarrollado una buena política de tratamiento de datos personales; en primer lugar tiene dos estatutos de protección de datos, uno se relaciona con la información crediticia – Ley 1266 de 2008 y el otro garantiza la protección de la información sobre una persona identificable registrada en archivos de datos, registros, banco de datos y otros medios técnicos- Ley 1581 de 2012. Juntos constituyen un régimen legal común que establece la protección de datos personales Montezuma Chávez (2018). En segundo lugar, ha definido los sujetos que intervienen en el proceso de tratamiento de datos. Ha clasificado de acuerdo a su naturaleza los datos de especial protección. Aspecto que anteriormente con la Ley 1266 de 2008 se tenía incertidumbre. Así mismo, ha suministrado los aspectos relevantes que deben ser tenidos en cuenta al momento de elaborar políticas en el tratamiento de Información. De igual manera, ha regulado expresamente y en detalle cómo debe ser obtenido de manera legal el consentimiento del titular a través de la elaboración de los formatos de autorización, ya que este es uno de los aspectos básicos y de mayor sensibilidad en el tratamiento de datos personales. En general cuenta con una legislación amplia y completa en materia de protección de datos.

Vale la pena aclarar que dicha normatividad y la jurisprudencia ha sido estructurada de manera progresiva de conformidad con el desarrollo que ha tenido Colombia en temas tecnológicos. Es decir, que la norma se ha ido ajustando de acuerdo a los avances informáticos, en aras de brindar seguridad frente al cúmulo de datos que a la fecha circulan en los diferentes canales y redes cibernéticas.

Por otro lado, se observa que el avance y la adaptación en temas de protección de datos no solo se ha ido presentando con los ajustes normativos, sino adicional a ello con la pedagogía de la norma, pues el Estado ha proporcionado a través de los entes encargados las capacitaciones respectivas en esta materia, de tal manera que las entidades o personas responsables o encargadas en el tratamiento de datos vayan ajustando sus políticas de acuerdo a las normas existentes. Así como también han efectuado ajustes en el personal designado para ello y han implementado los controles de seguridad que requiere el manejo de información.

Luego entonces es correcto afirmar que la política desarrollada en Colombia es efectiva, pues, además de desarrollar los aspectos normativos que este proceso requiere, el Estado a través de sus organismos ha suministrado las herramientas con las cuales se presta capacitación para ello. Lo anterior, en aras de velar por la efectiva y correcta administración de datos personales. Un tema que, si bien ha sido regulado de manera reciente, necesita una constante estructuración.

Así mismo, la Superintendencia de Industria y Comercio, además de ser una herramienta pedagógica, a través de la cual se pueda ir estructurando un modelo de protección de datos efectivo, también su facultad jurisdiccional, ha contribuido para que el proceso de regulación en dicha materia sea eficaz. En efecto, así lo expuso Cuevas Rodríguez (2015):

> De allí que Colombia diera un paso adelante y concediera dicha facultad de sancionar a una instancia administrativa como la Superintendencia de Industria y Comercio, pues es una disposición que agiliza los trámites relacionados con el tratamiento de los datos personales, protegiendo mejor los derechos de los titulares y poniendo en orden las operaciones de los terceros que los administran y garantizando un poco más de celeridad en la misma diligencia.

No obstante, si bien se ha incentivado las buenas prácticas respecto a la implementación de políticas de tratamiento de información, se observa que aún se presentan deficiencias en la aplicabilidad y la adaptabilidad de la norma por parte de las organizaciones, pues en algunos casos, el desconocimiento de la norma y la falta de personal especializado en el tema, hace que los responsables o los encargados en el tratamiento de datos personales omitan aspectos

importantes lo que genera errores en la adecuación de sus políticas y por lo tanto aparezcan riesgos en el cuidado y protección de la información. Luego entonces, no podría hablarse de una deficiencia en la política que actualmente Colombia presenta y desarrolla sino por el contrario una debilidad frente a la aplicabilidad de la norma en materia de protección de datos.

En ese orden de ideas, resultan ser debilidades prácticas mas no por ausencias o vacíos normativos.

Finalmente, el constante crecimiento y cambio frente al uso de nuevas tecnologías y herramientas informáticas hace que el nivel de riesgo respecto a la protección de datos vaya en constante crecimiento, pues hoy en día, el proceso de recolección, uso y administración de datos personales es una actividad habitual. Por lo tanto, las falencias que se presenten dentro de este proceso de tratamiento de datos no pueden ser adjudicada a la ineficacia de la norma o a la política de tratamiento de datos que actualmente se desarrolla en Colombia, sino por el contrario a la insuficiencia por parte de las organizaciones en la adaptación y ajuste de sus procedimientos en tema de datos personales de conformidad con las leyes emitidas en este tema.

3.4. Responsabilidad del Estado frente al tratamiento de datos Personales

Como se ha insistido dentro del presente escrito, la aparición de las nuevas tecnologías ha derivado que se presenten diversas situaciones que requieran de una especial atención y protección.

En primer lugar, se observa un tema comercial, el cual va ligado con el ofrecimiento de productos y servicios que buscan satisfacer las nuevas necesidades de la sociedad, las cuales han surgido con los cambios tecnológicos y cibernéticos. Es así como los grandes proveedores en materia de tecnología buscan que sus servicios se adapten a lo pretendido por los usuarios. Por consiguiente, se evidencian promociones en materia de servicios de internet, telefonía móvil y celular, aplicaciones, paquetes en los que se incluyan nuevos servicios, entre otros. Todo en aras de satisfacer los gustos de los clientes. Situaciones que han obligado al Estado a regular y a tener una responsabilidad frente a los proveedores de estos servicios, todo con el fin de garantizar la correcta prestación de los mismos a los usuarios.

Responsabilidad que tal y como lo han señalado Becerra, Cotino Hueso, García Vargas, Sánchez Acevedo y Torres Ávila (2015 a, p.179) se encuentra dirigida

> "al conjunto de políticas públicas, leyes y decretos que han creado en los últimos quince años en Colombia y que han contribuido a generar este conjunto de nuevas situaciones y relaciones jurídicas, que llevan a plantear el tema de la responsabilidad como un punto central del papel que juega y jugará el Estado a través de medios electrónicos."

Es por ello, que el Estado tiene una responsabilidad con los usuarios de dichos servicios y por lo tanto es su deber vigilar que la prestación de dichos servicios se haga en debida forma. Para lo cual, debe crear normatividad que regule estas relaciones, donde el objetivo primordial es garantizar y responder a los usuarios por la correcta prestación de un servicio.

En segundo lugar, se observa que más allá de velar por una correcta relación comercial entre ciudadanos y proveedores, El Estado tiene una Responsabilidad directa con los ciudadanos a que se les respeten sus garantías constitucionales en el marco de esa relación comercial, específicamente las relacionadas a los Derechos Fundamentales, que para el caso que nos ocupa el presente documento, son aquellas garantías relacionadas a la protección especial de los datos personales de los ciudadanos.

En efecto, se observa como dentro de esta relación en la que se comercializan productos derivados de nuevas tecnologías, los datos personales resultan ser un activo indispensable para la misma y por lo tanto los mismos deben gozar de especial protección por parte de los proveedores. Protección que como ya se ha explicado durante todo el escrito, prima en cabeza de los proveedores, pues son ellos, quienes a través de la aplicación de la normatividad vigente en materia de protección de datos deben garantizar el correcto uso y circulación de dichos datos.

Sin embargo, si bien el Estado tiene una responsabilidad frente a los proveedores en materia comercial, también existe una responsabilidad de parte del Estado directamente

relacionada con el respecto y cumplimiento de las garantías constitucionales de los ciudadanos. Es decir una Responsabilidad en sentido amplio, pues finalmente, los ciudadanos además de ser usuarios de los servicios adquiridos, son los titulares de la información y por ende gozan de una especial protección frente a su información. En ese sentido lo ha señalado Becerra, etal., (2015 b, p. 189) "les impone el deber de protección de los derechos de los usuarios, que aseguraría que exista una responsabilidad de los operadores, cuando no se actúe de manera adecuada en la protección de [sus] derechos"

Ahora bien, dicha responsabilidad de parte del Estado debe verse representada directamente en todas las normas vigentes que promulga, específicamente en materia de protección de datos, pues en estas, se estipulan todos los lineamientos que deben adoptar los proveedores de servicios que a su vez serán los encargados y responsables de efectuar tratamiento de datos personales. Luego entonces, la responsabilidad del Estado no solo debe velar porque estos grandes proveedores cumplan las normatividades en temas comerciales sino también que éstos en su relación comercial respeten y garanticen la prelación de los derechos fundamentales de los ciudadanos.

Así las cosas, la Responsabilidad del Estado debe estar dirigida en la elaboración de políticas públicas que garanticen el respeto de los derechos de los ciudadanos, así lo señaló Becerra (2015 c, p.196).

Conclusiones

De conformidad con los aspectos plasmados en el presente artículo, se extraen las siguientes conclusiones y reflexiones finales en torno a los principales postulados expuestos en la Ley Estatutaria 1581 de 2012 en materia de tratamiento de datos personales:

- Dada la cantidad de información que suministran los Datos Personales, ya que los mismos definen e identifican a las personas dentro entornos sociales, culturales, comerciales y/o financieros, es necesario que estos estén sujetos a una protección especial en cuanto a su recolección, administración y circulación, así lo ha señalado la Ley 1581 de 2012.

- Dentro del gran universo de los datos personales, para garantizar la disponibilidad, confidencialidad e integridad de la información personal recolectada. Así como también, el suministro de los mismos a terceros, las medidas de seguridad que estos requieren y el consentimiento para su tratamiento, es necesario que los datos se clasifiquen de acuerdo a su naturaleza. Para ello, la Ley Estatutaria 1266 de 2008 junto con la Ley 1581 de 2012, determinaron una clasificación específica de los datos en públicos, privados, semiprivados, sensibles y aquellos que están relacionados con los niños, niñas y adolescentes.

  No obstante lo anterior, resulta menester aclarar que la clasificación de los datos no es estática, por el contrario su connotación puede cambiar dependiendo del contexto del tratamiento.

- Colombia ha demostrado avances significativos en materia de protección de datos, pues goza de un amplio componente normativo y jurisprudencial en esta materia. En efecto, con la expedición de la Ley 1266 de 2008, se regularon todos los aspectos relacionados con el Habeas Data Financiero. Así como también, con la expedición de la Ley 1581 de 2012, su Decreto Reglamentario 1377 de 2013 y su sentencia de revisión Constitucional C-748 de 2011, se definieron todos los aspectos relacionados con los datos personales y las políticas de tratamiento a desarrollar por parte de las personas responsables o encargadas de efectuar tratamiento de datos.

- Ley 1581 de 2012 definió ocho principios rectores a través de los cuales se estructuraron los lineamientos fundamentales que deben ser tenidos en cuenta al momento de implementar y desarrollar una correcta política de tratamiento de datos personales, pues en los mismos se encuentran todas las pautas y las bases necesarias para atender los parámetros establecidos en la norma.

- Con la expedición de la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013, se adoptaron y desarrollaron mecanismos de seguridad que permitieran el correcto uso y circulación de los datos. Dentro de los mismos, se definió los alcances de la autorización. Ésta como medio de recolección y circulación de Datos Personales, resulta ser efectiva y garantista en el tratamiento de datos personales, pues a través del otorgamiento de la misma lo que se busca es contar con el consentimiento previo del titular respecto al uso, administración y circulación de sus datos, lo cual permite que el titular ejerza un control sobre su información personal. Adicional a ello, con el cumplimiento de dicho requisito se contribuye con el desarrollo de una buena política de tratamiento de información.

- Si bien la Ley 1581 de 2012 dentro de sus lineamientos no contempló el Principio de Responsabilidad Demostrada, el Decreto reglamentario 1377 de 2013 si lo materializó. A través de este, se desarrollaron de manera explícita cada uno de los componentes de dicho principio, lo cual, trajo consigo un avance significativo en materia de protección de datos, pues con la implementación del mismo, se permitió que las personas dedicadas a hacer tratamiento de datos personales desarrollaran y estructuraran una correcta política de tratamiento de información, en la cual, se hiciera un seguimiento en la operación que se desarrolla en este proceso, se identifiquen los posibles riesgos a los que se ve expuesta la información y por consiguiente se diseñen y se adopten medidas efectivas que permitan cumplir con estándares de calidad en el manejo de la información.

- Con la expedición del Decreto reglamentario 1377 de 2013, lo que se buscaba era enfatizar en aspectos particulares propios de la administración y tratamiento de los datos personales que no fueron objeto de discusión en la Ley 1581 de 2012, como es el caso del principio de

accountability o de Responsabilidad Demostrada. Con la definición del mismo, se buscó que las empresas bajo la aplicación de éste, desarrollaran programas de protección de datos o sistemas de gestión de protección de datos con el objetivo de cumplir con la normatividad vigente en esta materia, específicamente en lo que respecta a la calidad y la seguridad de la información.

- Dentro de los aspectos expuestos en La Ley 1581 de 2012, se observa que dicha normatividad no solo se encargó de regular los procedimientos necesarios para un correcto tratamiento de información, sino adicionalmente, destacó la importancia de la partición de aquellos Responsables y Encargados en el manejo de los datos, pues los mismos, tendrían como función principal velar porque las políticas adoptadas en materia de protección de datos se cumplan a cabalidad. Ello a través del desarrollo de medidas reales y eficaces que garanticen una protección adecuada de los datos objeto de tratamiento.

- La Ley Estatutaria 1581 de 2012 es efectiva y garantiza la protección de los datos personales de los titulares, pues en la misma se han expuesto los lineamientos necesarios sobre los cuales deben desarrollarse políticas efectivas en el tratamiento de la información, a través de las cuales se le permita al titular conocer de una manera clara, rápida y constante las finalidades por las cuales fueron recolectados sus datos, el tratamiento al cual fueron sometidos, los datos de contacto del responsable o el encargado, las funciones que dichos sujetos desempeñan dentro de tal proceso, los canales de consultas y reclamos, y en general todos los aspectos relacionados al uso y administración de sus datos personales. Claramente en cumplimento neto al principio de transparencia.

- El Estado debe velar porque los servicios adquiridos por parte de los usuarios se presten en correcta forma por parte de los proveedores. Sn embargo, esta responsabilidad no solo debe ser encaminada a la protección de aspectos comerciales sino adicional a ello, también debe velar porque las garantías constitucionales de los usuarios, sean respetadas a través de la aplicación de las normas vigentes que regulen dichas actuaciones.

Referencias:

Agencia Española de Protección de Datos. *Estándares Internacionales sobre Protección de Datos Personales y Privacidad (2009).* Recuperado de https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf

Bautista Avellaneda, M. E. (2015). *Marco constitucional y jurisprudencia constitucional del derecho a la intimidad*. En: M. E. Bautista Avellaneda. El derecho a la intimidad y su disponibilidad pública (pp. 29-38). Bogotá: Universidad Católica de Colombia

Bautista Avellaneda, M. E. (2015). M*arco legal en Colombia, la Ley Estatutaria de Protección de Datos y el tratamiento penal*. En: M. E. Bautista Avellaneda. El derecho a la intimidad y su disponibilidad pública (pp. 41-51). Bogotá: Universidad Católica de Colombia

Becerra, J., Sánchez Acevedo, M. E., Torres Ávila, J., García Vargas, C. B. & Cotino Hueso, L. (2015). *El derecho a la protección de datos personales y la responsabilidad de la administración pública en el tratamiento de datos personales*. En J. Becerra, M. E. Sánchez Acevedo, J. Torres Ávila, C. B. García Vargas & L. Cotino Hueso. (2015). La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC). Bogotá: Editorial Universidad Católica de Colombia.

Cerda Silva, A. (2003). Autodeterminación informativa y leyes sobre protección de datos.*Revista Chilena de Derecho Informático,* (3). doi:10.5354/0717-9162.2011.10661

Comisión Europea. (2018). *¿Qué son los datos personales?* Recuperado de https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

Comisión Europea. Grupo de Trabajo de Protección de Datos del Artículo 29: *Dictamen 3/2010. (2010). Recuperado de* https://sontusdatos.org/wp-content/uploads/2013/04/ce-dictamen-3-2010-principio-de-responsabilidad.pdf

Congreso de Colombia. (18 de octubre de 2012) Artículo 3 [Titulo I]. Ley Estatutaria [ley 1581 de 2012]. DO: 48.587

Congreso de Colombia (31 de diciembre de 2008) Artículo 3. Ley Estatutaria [Ley 1266 de 2008]. DO: 47.219

Corte Constitucional (01 marzo de 1995) Sentencia SU-082 de 1995 [MP Jorge Arango Mejía]

Corte Constitucional, (06 de octubre de 2012) Sentencia C-748 2012 [MP Jorge Ignacio Pretelt Chaljub]

Corte Constitucional (05 de septiembre de 2012) Sentencia T-729 DE 20012 [MP Eduardo Montealegre Lynett]

Cuevas Rodríguez, M. P. (2015). *De la protección de datos personales en Colombia (Ley 1581 de 2012): un estudio comparado con el sistema canadiense*. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia

Ducuara Cuervo, C. A. & Soto Espinosa, C. C. (2018). *Protección de datos personales en los servicios de internet*. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia

Fernández Pedrosa, J. A. (2017). *Guía de implementación y lecciones aprendidas para el proyecto de aplicación de la Ley de Protección de Personales. Caso: Fiduprevisora S.A*. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería Industrial. Bogotá, Colombia

Garriga, A. (2004). *Tratamiento de Datos Personales y Derechos Fundamentales*. Madrid, España: Dykinson S.L.

Galvis Cano, L. (2012) Revista Lebret. *Protección de Datos en Colombia Avances y Retos*, (4), 195-214. Recuperado de http://revistas.ustabuca.edu.co/index.php/LEBRET/article/view/336/336

Martínez Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. *IDP. Revista de Internet, Derecho y Política*, (5), 47-61. Recuperado de http://www.redalyc.org/html/788/78812861005/

Ministerio de Comercio Industria y Turismo. (27 de junio de 2013) Decreto Reglamentario. [Decreto 1377 de 2013]. DO. 48834

Montezuma, L. (2018). IAPP: Privacy pespectives: *Obtaining adequacy standing for Colombia*. Recuperado de https://iapp.org/news/a/obtaining-adequacy-standing-for-colombia/

Observatorio Iberoamericano de Protección de Datos. (2013). Iniciativa sobre privacidad, protección de datos y habeas data en Iberoamérica. Recuperado de http://oiprodat.com/2013/04/15/principios-rectores-del-tratamiento-de-datos-personales/

Pérez Fernández, O. E. (2017). *El habeas data en Colombia: su desarrollo y conexidad con los derechos fundamentales*. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia

Pfeiffer, M. (2008). Derecho a la privacidad. Protección de los datos sensibles. *Revista Colombiana de Bioética*, *3* (1), 11-36.

Puyol, J (12 de febrero de 2017). Confilegal. Recuperado de https://confilegal.com/20170212-consiste-llamado-principio-responsabilidad-demostrada/

Quiroga, A (26 de septiembre de 2014). Asuntos: legales. Recuperado de https://www.asuntoslegales.com.co/analisis/andres-felipe-quiroga-511176/aplicacion-del-principio-de-responsabilidad-demostrada-2173831

Red Iberoamericana de Protección de Datos (mayo de 2006). *Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana.* Trabajo presentado en la reunión celebrada en Santa Cruz de la Sierra, Bolivia

Remolina Angarita N (julio-diciembre 2012). Aproximación constitucional de la protección de datos personales en Latinoamérica. *Revista Internacional de Protección de Datos Personales.* Recuperado de https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf

Remolina Angarita, Nelson. Álvarez Zuluaga, Luisa Fernanda. (2018). *Guía GECTI para la implementación del principio de responsabilidad demostrada –accountability– en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos*. Universidad de los Andes (Bogotá, Colombia). Facultad de Derecho. GECTI, 1-58.

Remolina Angarita N, *¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?*, 16. International Law, Revista Colombiana de Derecho Internacional, 489-524 (2010)

Remolina Angarita, N. (2013). *Tratamiento de datos personales*. 1a ed. Bogotá, Colombia: Legis

Reglamento (Ue) 2016/679 del Parlamento Europeo y del Consejo (27 de abril de 2016). [l 119/1] do: 4.5.2016. ES

Rojas Bejarano, M. (2014). *Evolución del Derecho de Protección de Datos Personales en Colombia respecto a Estándares Internacionales*. Novum Jus, 8 (1), 107-139. Doi: http://dx.doi.org/10.14718/NovumJus.2014.8.1.6

Ruiz Ardila, B. J. (2016). *Regulación en materia de protección de datos personales o habeas data en Colombia a través de la Ley 1581 de 2012: examen histórico y crítico sobre su ineficacia ante las administradoras de bases de datos, portales de Internet y motores de búsquedas*. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia

Superintendencia de Industria y Comercio. *Cartilla de formatos modelo para cumplir la Ley 1581 de 2012.* (2017). Recuperado de http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_formatos_datos_Personales_nov22.pdf

Superintendencia de Industria y Comercio. Protección de Datos Personales: *Aspectos prácticos Sobre el Derecho de Habeas Data. (2016). Recuperado de* http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Aspectos_Derecho_de_Habeas_Data.pdf

Superintendencia de Industria y Comercio. *Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability)*. (2015). Recuperado de https://issuu.com/quioscosic/docs/guia_accountability_26_p__g

Superintendencia de Industria y Comercio. *Sobre la Protección de datos personales (2016).* Recuperado de http://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Viega, M.J. (2010)._Los Principios Jurídicos En La Protección de Datos Personales [Entrada de blog] Recuperado de: http://mjv.viegasociados.com/wp-content/uploads/2011/05/Analisis-comparativo-de-principios.pdf

Woolcott, O., Monje, D., Peláez, H., Comandé, G. y Alarcón, A. (2018). *Estudios contemporáneos de derecho privado. Responsabilidad civil, propiedad, contratos y obligaciones*. Bogotá: Editorial Universidad Católica de Colombia.

ANEXO 01

Tabla 1

Normatividad y Jurisprudencia existente en materia de Habeas Data Financiero

Norma	Fecha de Expedición	Corporación que la expidió	Aspectos regulados
Ley 1266 de 2008	31 de diciembre de 2008	Congreso de la República	En dicha normatividad se desarrollaron todos los aspectos relacionados con la recolección, circulación y administración de información comercial y financiera ante las bases de datos los operadores de la información.
Sentencia C-1011 de 2008	16 de octubre de 2008	Corte Constitucional	Control Constitucional de la Ley 1266 de 2008 (Declaró la Exequibilidad de la Norma)
Decreto 1729 de 2009	15 de mayo de 2009	Ministerio de Comercio, Industria y Turismo	Se reguló la forma en la cual los operadores de los bancos de datos debían presentar la información.
Decreto 2952 de 2010	06 de agosto de 2010	Ministerio de Comercio, Industria y Turismo	Se desarrollaron los artículos 12 (requisito de comunicación previa) y 13 (Termino de permanencia de la información) de la Ley 1266 de 2008. Así mismo se reguló el reporte de información negativa en los casos de fuerza Mayor o caso Fortuito.
Resolución 76434 de 2012	04 de diciembre de 2012	Superintendencia de Industria y Comercio	Por la cual se deroga el contenido del Título V de la Circular Única de la Superintendencia de Industria y Comercio, sobre Acreditación, y se imparten instrucciones relativas a la protección de datos personales, en particular, acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, las cuales se incorporan en el citado Título.

Fuente: Elaboración propia

ANEXO 02

Tabla 2

Normatividad y Jurisprudencia existente en materia de Protección de Datos Personales

Norma	Fecha de Expedición	Corporación que la expidió	Aspectos regulados
Ley 1581 de 2012	17 de octubre de 2012	Congreso de la República	En dicha normatividad se desarrollaron todos los aspectos relacionados con el tratamiento y protección de datos personales
Sentencia C-748 de 2011	6 de octubre de 2011	Corte Constitucional	Control Constitucional de la Ley 1266 de 2008 (Declaró la Exequibilidad de la Norma)
Decreto 1377 de 2013	27 de junio de 2013	Ministerio de Comercio, Industria y Turismo	Se regularon aspectos relacionados con: (i) autorización para circulación de datos; (ii) funciones y deberes de los Responsables y Encargados del tratamiento de datos; y (iii) transferencia a terceros países de datos personales.
Decreto 886 de 2014	13 de mayo de 2014	Ministerio de Comercio, Industria y Turismo	Se reguló todo el trámite de registro nacional de base de datos

Fuente: Elaboración propia