Prôtegis data[1]

María Fernanda De la Ossa Archila[2]
María Carolina Corcione Morales[3]

RESUMEN

El suministro de datos personales por los particulares se realiza casi a diario, por lo que es básico conocer quién tiene esos datos, cuáles son las medidas que adopta este sujeto para que dichos datos sean utilizados de manera correcta y para unos fines precisos para los cuales se han suministrado. La pregunta concreta que debe uno formularse es cómo se protegen los datos personales. Teniendo en cuenta lo anterior, en este artículo se hará un recuento de lo que ocurre en el contexto colombiano, en donde el legislador, por medio de la Ley 1581 de 2012 que fue sometida a control previo de constitucionalidad, reguló los derechos de los titulares de la información, los deberes de los responsables y encargados del tratamiento de la información suministrada y señaló de manera concreta cuál es la autoridad encargada para la vigilancia y control de una efectiva protección de los datos personales.

Palabras clave: Derecho público, Vida privada, Derecho a la intimidad, Datos personales, Superintendencia de Industria y Comercio.

Prôtegis data

ABSTRACT

Throughout our lives, and almost daily, we provide our personal data to strangers in order to acquire goods, have access to different services or to carry

1 Fecha de recepción del artículo: septiembre 10 de 2013; fecha de modificación del artículo: 4 de octubre de 2013; fecha de aceptación del artículo: 1 de noviembre de 2013. Para citar el artículo: De la Ossa Archila, María Fernanda y María Carolina Corcione Morales (2013). "Prôtegis data", en *Revista Digital de Derecho Administrativo* Nº 10. Bogotá: Universidad Externado de Colombia, pp. 111-143.

2 Abogada de la Universidad Externado de Colombia, especialista en Derecho Contractual y Relaciones Jurídico Negociales de la misma. Abogada asociada de VGCD Abogados. Consultora del Proyecto de Asistencia Técnica al Comercio de la Unión Europea. Correo-e: mdelaossa@vgcd.co

3 Abogada de la Universidad Externado de Colombia con maestría de la Universitá degli studi di Roma Tor Vergata. Directora de Investigaciones de Protección al Consumidor de la Superintendencia de Industria y Comercio. Profesora de cátedra de Derecho Romano de la Universidad de Los Andes. Correo-e: mc.corcione179@uniandes.edu.co

on transactions within public or private entities. We find ourselves revealing our intimacy to the supermarket cashier, the saleswoman in a clothing store, a bank adviser, the State, among others. Therefore, we need to know who has this information, what are the measures taken to assure that the data is being used correctly and for the specific purposes for which it was supplied. The specific question that should be asked is how to protect personal data. Given the above, this article will illustrate about what happens in the Colombian context, where the1581 Act of 2012, which was subject to prior control of constitutionality, regulates the rights of holders of information, the duties of the Officers and Managers of treatment and the authority responsible for the supervision and control of effective protection of personal data.

Keywords: Public law, Private life, Right to privacy, Personal data, Superintendence of Industry and Comerce.

1. LA PROTECCIÓN DE DATOS PERSONALES

A lo largo de nuestras vidas suministramos nuestros datos personales para poder adquirir bienes, acceder a la prestación de un servicio o para adelantar cualquier tipo de trámite bien sea ante una entidad pública o privada. Suministramos nuestros nombres y el de nuestros familiares, direcciones de residencia, teléfonos, direcciones de correo electrónico, entidades financieras en las cuales tenemos algún tipo de producto e incluso, llegamos a informar cuáles son nuestros *hobbies* y las actividades que practicamos en nuestro tiempo libre; sin contar aquellos datos que se recaudan durante el desarrollo de investigaciones por parte de organismos estatales. Se encuentra uno haciéndole un pequeño recuento de su intimidad al cajero de un supermercado, a la vendedora en un almacén de ropa, al asesor de un banco, al Estado, entre otros. La pregunta que nos debe resultar obligatoria luego de cuestionarnos acerca de quién tiene esos datos, es cuáles son las medidas que adopta este sujeto para que dichos datos sean utilizados de manera correcta y para unos fines precisos para los cuales los han sido suministrados. La pregunta concreta que debe uno formularse es cómo se protegen los datos personales.

La protección de datos personales está estrechamente vinculada al derecho fundamental a la intimidad previsto en el artículo 15 de la Constitución Política de 1991[4]. No obstante, el derecho al *habeas data* o la protección de datos

4 Este dispone: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. *De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.* En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o

personales es un derecho autónomo[5] que, tal como lo ha precisado la Corte Constitucional, tiene el carácter de fundamental y "otorga la facultad al titular de los datos personales de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación, o cesión de los mismos conforme a los principios que informan el proceso de administración de datos personales"[6].

En sentencia C-1011 de 2008, la misma Corte reconoció la autonomía del derecho al *habeas data* al precisar que "el derecho al *habeas data* confiere un grupo de facultades al individuo, para que en ejercicio de la cláusula general de libertad, pueda controlar la información que de sí mismo ha sido recopilada en una central de información. En este sentido este derecho fundamental está dirigido a preservar los intereses del titular de la información ante el potencial abuso del poder informático".

En relación con el uso del poder informático, tema asociado de manera estrecha a la protección de datos personales, la Corte Constitucional, en las

registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley".

5 Corte Constitucional, Sentencia T-260 de 2012: "El artículo 15 de la Constitución de 1991 reconoció explícitamente el *"(…) 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"* y además dispuso que *"[e]n la recolección, tratamiento y circulación de datos se respetará la libertad y demás garantías consagradas en la Constitución"*. Estos preceptos leídos en conjunto con la primera parte del mismo artículo 15 –sobre el derecho a la intimidad, el artículo 16 –que reconoce el derecho al libre desarrollo de la personalidad– y el artículo 20 –sobre el derecho a la información activo y pasivo y el derecho a la rectificación– de la Carta, *han dado lugar al reconocimiento de un derecho fundamental autónomo catalogado como derecho al habeas data, y en algunas oportunidades, como derecho a la autodeterminación informativa o informática"* (resaltado fuera del texto).

6 Corte Constitucional, Sentencia T-729 de 2009.
Cfr. Corte Constitucional Sentencia T-444 de 1992: "El habeas data, es el derecho de obtener información personal que se encuentre en archivos o bases de datos. Este derecho implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos. Con este derecho se pretende proteger la intimidad de las personas ante la creciente utilización de información personal por parte de la administración pública, de entidades financieras, educativas, profesionales u otras organizaciones privadas. Lo importante es que las personas no pierdan el control sobre la propia información, así como sobre su uso.
(…)
Este derecho establece una doble línea de salvaguarda de los particulares; por una parte, incorpora obligaciones exigibles a entidades públicas y privadas que recopilan y tratan información, tales como de regirse por principios de lealtad, legitimidad con relación a la finalidad para lo que se recolectarán los datos. Y por otra parte consiste en el derecho que tiene toda persona a exigir del Estado el respeto a derechos como el de la intimidad personal y familiar y a su buen nombre".

sentencias T-414 de 1992 y C-1066 de 2008, ha precisado que se trata de un fenómeno que está en la médula de la función jurídico social de la administración de bases de datos de carácter personal. Así, la citada corporación manifestó que "frente al robustecimiento de dicho poder, característico de la sociedad de la información, el *habeas data* surge como un cuerpo normativo singular orientado a proteger las libertades individuales. Dada la existencia extendida de bases de datos de carácter personal, magníficas condiciones de interconexión y accesibilidad, y posibilidades de uso en tiempo real, el *habeas data* es la respuesta del constitucionalismo para enfrentar las amenazas que el ejercicio inorgánico de este poder supone para la libertad de los seres humanos"[7].

A partir de la descripción que la jurisprudencia ha hecho del derecho fundamental, dentro de las prerrogativas que se desprenden del derecho al *habeas data* se encuentran: (i) el derecho de las personas a conocer o acceder a la información que sobre ellas está recogida en bases de datos –lo que conlleva el acceso a la bases de datos donde se encuentra dicha información–; (ii) el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir a poner al día el contenido de dichas bases de datos, y (iv) el derecho a excluir información de una base de datos bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular, salvo las excepciones previstas en la ley.

2. EL MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS PERSONALES

Precisado el alcance y la naturaleza del derecho al *habeas data*, es necesario visualizar cuál ha sido el desarrollo legislativo que ha tenido este derecho en Colombia a partir de su consagración constitucional.

Sea lo primero advertir que antes de la inclusión expresa del derecho al *habeas data* en la Constitución Política de 1991, el tema de la protección de datos había ya sido materia de regulación en importantes escenarios internacionales, como lo son la Organización para la Cooperación y el Desarrollo Económico[8],

7 Cfr. Corte Constitucional Sentencia SU-082 de 1995 en donde la Corte basó toda *la ratio decidendi*, en el concepto de autodeterminación informática, cuyo elemento esencial recaía en el consentimiento. Sobre el particular, la Corte se preguntó: "¿Cuál es el núcleo esencial del habeas data? A juicio de la Corte, está integrado por el derecho a la autodeterminación informática y por la libertad, en general, y en especial económica. La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales". Esa posición ha sido reiterada, entre muchas otras, en las sentencias T-580 de 1995, T-448 de 2004, T-526 de 2004, T-657 de 2005, T-T-684 de 2006, C-1011 de 2008, T-017 de 2011.

8 Organization por Economic Cooperation and Development (1980).

la Organización de las Naciones Unidas[9] y la Unión Europea[10], en las cuales se sentaron los principios a aplicar en el manejo y protección de la información personal almacenada por el sector público o privado, ya sea que por la forma como fue procesada, por su delicada naturaleza o por el contexto en el cual es usada, presenten un riesgo para la privacidad y las libertades individuales.

En Colombia, luego de múltiples pronunciamientos jurisprudenciales al respecto, el legislador decidió promulgar la Ley Estatutaria 1266 de 2008, "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones". La Ley 1266 de 2008, entre otros aspectos, reguló el tratamiento de los datos de carácter financiero, crediticio y comercial, y en ella se definieron y delimitaron los derechos de los titulares y los deberes de los operadores, de las fuentes de información y de los usuarios de la misma. Definió lo que es el dato público, el privado, y el semiprivado, e incluyó dentro de este último el dato financiero y crediticio. Dentro de los aspectos destacables de la ley se encuentran los deberes que se imponen tanto a los operadores de la información como a las fuentes y usuarios de la misma. Estos deberes están dirigidos a proteger a los titulares de la información y a brindarles los mecanismos para su defensa.

Posteriormente, se expidió la Ley 1273 de 2009, "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado 'de la protección de la información y de los datos'– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Mediante dicha ley, se adicionó al Código Penal el Título VII BIS denominado "De la Protección de la información y de los datos", en el que se incluyen tipos penales, como el acceso abusivo a un sistema informático, la obstaculización ilegítima de sistema informático o red de telecomunicación, la interceptación de datos informáticos, el daño informático, el uso de *software* malicioso, la violación de datos personales y la suplantación de sitios web para capturar datos personales, entre otros.

Recientemente, y luego del respectivo control previo de constitucionalidad efectuado por la Corte Constitucional mediante Sentencia C-748 de 2011, se promulgó la Ley estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales". Esta ley introduce principios y reglas generales destinadas a garantizar el contenido mínimo del citado derecho.

En efecto, la Ley 1581 de 2012 es una reglamentación de carácter general aplicable a todos los datos personales que, tal como quedó consignado en su

9 Organización de las Naciones Unidas (1990).

10 Unión Europea - Parlamento Europeo y el Consejo de la Unión Europea (1995).

exposición de motivos, responde a la necesidad de que "(…) el país cuente con una legislación integral y transversal que garantice la protección efectiva de los datos personales en todo el proceso de tratamiento".

Sobre el carácter general de la Ley 1581 de 2012, en la sentencia antes citada, la Corte Constitucional precisó que "con la introducción de esta reglamentación general y mínima aplicable en mayor o menor medida a todos los datos personales, el legislador ha dado paso a un sistema híbrido de protección en el que confluye una ley de principios generales con otras regulaciones sectoriales, que deben leerse en concordancia con la ley general, pero que introduce reglas específicas que atienden a la complejidad del tratamiento de cada tipo de dato"[11].

En consideración a lo anterior, resulta claro que las disposiciones contenidas en la hasta ahora única ley estatutaria en la materia, esto es, la Ley 1266 de 2008, deben ser interpretadas y aplicadas teniendo en cuenta los principios y reglas generales introducidos por la Ley 1581 de 2012, que para todos los efectos constituye el marco general de protección de los datos personales.

Adicionalmente se advierte que las disposiciones consagradas en la Ley 1266 de 2008, especialmente las relacionadas con las reglas para el reporte de información negativa a centrales de riesgo y permanencia de los datos negativos, coexisten con las disposiciones de Ley 1581 de 2012 y deben ser observadas a cabalidad por quienes ostenten la calidad de responsables de los datos. Deben mantenerse las reglas dispuestas para el cumplimiento de los deberes incluidos en la referida ley, en especial los relacionados con actualización de la información y caducidad del dato negativo conforme lo dispuso el artículo 13 de la ley en la interpretación dada por la Corte Constitucional con ocasión del control de la ley estatutaria[12].

3. LA LEY 1581: MARCO GENERAL DE PROTECCIÓN DE DATOS PERSONALES

3.1 Ámbito de aplicación del marco general de protección de datos personales

De conformidad con lo establecido en el artículo 12 de la Ley 1581 de 2012, *"Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.* La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del

11 Corte Constitucional, Sentencia C-748 de 2011.

12 Corte Constitucional, Sentencia C-1011 de 2008.

Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales" (resaltado fuera del texto)

De acuerdo con lo anterior, es claro que la aplicación de las disposiciones de la Ley 1581 de 2012 está sujeta a la verificación de tres condiciones previstas en el artículo 2, esto es, (i) la existencia de datos personales, (ii) registrados en una base de datos que los haga susceptibles de tratamiento y (iii) el responsable puede ser una entidad pública o privada.

En tanto concurran las citadas condiciones, el responsable del tratamiento[13] de los datos deberá dar cabal aplicación a las disposiciones contenidas en la Ley 1581 de 2012.

3.1.1 Los datos personales

Dispone la Ley 1581 en su artículo 3 que el titular de un dato es aquella persona natural cuyos datos personales sean objeto de tratamiento. Ahora bien, antes de entrar a precisar el alcance de lo que se debe entender por tratamiento, es necesario entender qué es un dato.

La Ley 1581 en su artículo 3 señala que por dato personal debe entenderse cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

La citada ley, dentro de la categoría general, dispone en el artículo 5 que existen unos datos sensibles, es decir, 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.

Por su parte, en el Decreto 1377 de 2013 encontramos la complementación de la clasificación de los datos personales prevista por la Ley 1561, en la medida en que dicha ley dispone que existen datos públicos, privados y semiprivados, derivando para cada uno de ellos una consecuencia distinta[14].

13 Ley 1581 de 2012, artículo 3: "Para los efectos de la presente ley, se entiende por:
"e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos".

14 Esta clasificación ya venía contemplada en la Ley 1266, artículo 3, literal e) "Dato Personal: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados".

El dato público, según lo indica la citada norma, es 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, los que no estén sometidos a reserva y los relativos al estado civil de las personas.

Por otra parte, es semiprivado el dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que refiera dicha ley.

Por último dispone que un dato privado es aquel que por su naturaleza íntima o reservada solo es relevante para el titular.

3.1.2 Las bases de datos

Dispone la Ley 1581, en su artículo 3, que una base de datos es un conjunto organizado de datos personales que sea objeto de tratamiento.

Resulta oportuno mencionar que la Corte Constitucional precisó que la aplicación de la nueva ley estatutaria no está determinada solo por la existencia de bases de datos, pues los archivos son una clase de base de datos en las que es posible conservar datos personales. En este sentido, el alto tribunal, en sentencia C-748 de 2011, que examinó la constitucionalidad de la Ley 1581 de 2012, manifestó que "los archivos –para efectos exclusivamente del proyecto–, en tanto son (i) depósitos ordenados de datos, incluidos datos personales, y (ii) suponen, como mínimo, que los datos han sido recolectados, almacenados y, eventualmente, usados mediante modalidades de tratamiento, son una especie de base de datos que contiene datos personales susceptibles de ser tratados y, en consecuencia, serán cobijados por la ley una vez entre en vigencia. Esta parece además haber sido la intención del legislador estatutario, toda vez que varios artículos del proyecto se refieren a los archivos como sinónimos de bases de datos o modalidades del mismo género al que pertenecen las bases de datos".

Por otra parte, el régimen de protección de datos personales que se establece en la Ley 1581, no será de aplicación:

a) *A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico*[15], explicando que cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al titular y solicitar su autorización.

15 De acuerdo con lo indicado en el Decreto 1377 de 2013, artículo 3, el ámbito personal o doméstico comprende aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales.

b) *A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional*, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.

c) *A las bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia*[16].

d) *A las bases de datos y archivos de información periodística y otros contenidos editoriales*. En efecto, tal como manifestó la Corte Constitucional mediante sentencia C-748 de 2011, "el literal d) del artículo 2 pretende evitar que las bases de datos y archivos de carácter periodístico se vean sometidos a los mismos límites que la información general, lo que podría traducirse en una limitación desproporcionada de la libertad de prensa, e incluso en censura –piénsese por ejemplo en la posibilidad de la obligación de revelar las fuentes. No obstante, debe esta Sala reiterar que en razón de la especial consideración que el constituyente otorgó a la libertad de expresión, las posibles colisiones con el derecho al habeas data deben ser resueltas por una regulación especial".

Sobre la naturaleza de estas bases de datos, esto es, respecto de la cuales no resultan aplicables las reglas contenidas en la Ley 1581 de 2012, la Corte Constitucional advirtió que "las bases de datos a las que se refiere el literal d) del artículo 2, *son aquellas de contenido eminentemente periodístico, y no aquellas que están en poder del medio de comunicaciones en virtud de otras actividades, como aquellas encaminadas a fines comerciales o publicitarios. Así, las bases de datos con la información de los suscriptores de un periódico sí estarán sujetas a la regulación de la futura ley estatutaria*[17]" (resaltado fuera del texto).

Ahora bien, debe aclararse que el denominado "derecho del olvido" al que hace alusión la sentencia SU-458 de 2012 de la Corte Constitucional y que supone la supresión completa de un dato personal incluido en una base datos, en nuestro concepto, no resulta aplicable a la información contenida en bases de datos y archivos de carácter periodístico, pues tal

16 En Sentencia T-444 de 1992, la Corte Constitucional en el caso de una mujer que había sido catalogada como rebelde e integrante de un grupo guerrillero y cuya solicitud era pedirle al juez que ordenara a los organismos de inteligencia del Estado la rectificación de la información recogida y la protección de su buen nombre, dispuso: "Los organismos de seguridad del Estado, internamente, pueden y deben contar con toda la información necesaria para el normal, adecuado, eficiente, legítimo y democrático ejercicio de su función de servicio a la sociedad civil y defensa del orden público y de las instituciones. Pero, eso sí, dichas instancias estatales no pueden difundir al exterior la información sobre una persona, salvo en el único evento de un "antecedente" penal o contravencional, el cual permite divulgar a terceros la información oficial sobre una persona. Por "antecedente" debe considerarse única y exclusivamente las condenas mediante sentencia judicial en firme al tenor del artículo 248 constitucional. Esta regla se predica, entre otros efectos, para los certificados sobre conductas y antecedentes".

17 Corte Constitucional, Sentencia C-748 de 2011.

información, tal como se acaba de señalar, está expresamente excluida del ámbito de aplicación de la Ley 1581 de 2012.

e) *A las bases de datos y archivos regulados por la ya vista Ley 1266 de 2008.*

f) *A las bases de datos y archivos regulados por la Ley 79 de 1993*, "Por la cual se regula la realización de los Censos de Población y Vivienda en todo el territorio nacional".

Es necesario precisar que si bien la ley establece que el régimen de protección de datos no se aplicará a las apenas citadas bases de datos, los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas.

3.1.3. El tratamiento de los datos y sus responsables

Por tratamiento de los datos debe entenderse cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión[18].

Tal como lo advirtió la Corte Constitucional en la ya tantas veces citada sentencia C-748 de 2011, "cuando el proyecto se refiere al *tratamiento*, hace alusión a cualquier operación que se pretenda hacer con el dato personal, con o sin ayuda de la informática, pues a diferencia de algunas legislaciones, la definición que aquí se analiza no se circunscribe únicamente a procedimientos automatizados. *Es por ello que los principios, derechos, deberes y sanciones que contempla la normativa en revisión incluyen, entre otros, la recolección, la conservación, la utilización y otras formas de procesamiento de datos con o sin ayuda de la informática.* (....) Lo que se pretende con este proyecto *es que todas las operaciones o conjunto de operaciones con los datos personales quede regulada por las disposiciones del proyecto de ley en mención*, con las salvedades que serán analizadas en otro apartado de esta providencia" (resaltado fuera del texto).

De acuerdo con lo anterior, es claro que las actividades de recolección, almacenamiento, uso, circulación o supresión de datos personales que se adelantan a través de cualquier medio, tecnológico o manual, para la concreción de nuevas actividades o para la consecución de proveedores o clientes, están sometidas a la observancia de las disposiciones previstas en la Ley 1581 de 2012, independientemente de que la información que reposa en bases de datos o archivos se haya recopilado antes de la entrada en vigencia de la norma.

En los literales d) y e) del artículo 3 de la Ley 1581 de 2012 se hace expresa mención al encargado y al responsable del tratamiento de los datos, respectivamente. Así, el responsable del tratamiento es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre

18 Ley 1561 de 2012. Artículo 3.

la base de datos y/o el tratamiento de los datos, mientras que el encargado del tratamiento es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento. La diferenciación de estos dos sujetos es necesaria para establecer el ámbito de sus deberes, enumerados en el título VI de la ley y constituye, a su a vez, una garantía para el titular del dato, que puede conocer quién es obligado a cumplir diferentes prerrogativas que se desprenden del *habeas data*[19].

Al respecto, vale la pena tener en cuenta el pronunciamiento de la Corte Constitucional en la mencionada sentencia C-748 de 2011 en cuanto precisó que "todos los principios de la administración de datos personales identificados en este proyecto –los cuales serán estudiados en otro acápite– *son oponibles a todos*

19 Corte Constitucional, Sentencia C-748 de 2011: "vale la pena advertir que el encargado del tratamiento no puede ser el mismo responsable, pues se requiere que existan dos personas identificables e independientes, natural y jurídicamente, entre las cuales una –el responsable– le señala a la otra –el encargado– cómo quiere el procesamiento de unos determinados datos. En este orden, el encargado recibe unas instrucciones sobre la forma como los datos serán administrados". Es necesario poner de presente que la Ley 1266 de 2008 consagra una estructura subjetiva diferente frente al tratamiento de datos personales. En su artículo 3 encontramos los siguientes sujetos: Titular de la información. Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley; Fuente de información. Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos; Operador de información. Se denomina operador de información a la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley. Por tanto el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente. Usuario. El usuario es la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos".

los sujetos involucrados en el tratamiento del dato, entiéndase en la recolección, circulación, uso, almacenamiento, supresión, etc., sin importar la denominación que los sujetos adquieran, es decir, llámense fuente, responsable del tratamiento, operador, encargado del tratamiento o usuario, entre otros" (resaltado fuera del texto).

3.2 Los principios que irradian el marco general de protección de datos

La Ley 1581 de 2012 tiene como fundamento axiológico los siguientes principios[20]:

1. *Principio de legalidad*: el titular tiene derecho a que sus datos sean tratados de conformidad con los límites establecidos en la normatividad vigente, en especial tomar acciones cuando su tratamiento esté expresamente prohibido. Significa también que todo lo relacionado con el tratamiento de datos personales está sometido a las reglas definidas por la ley, reglas que por su propia naturaleza resultan ser imperativas y no admiten convención o pacto en contrario.
2. *Principio de finalidad*: el titular tiene el derecho a ejercer un control constante sobre el dato, con el fin de determinar si el mismo está siendo utilizado para fines legítimos y respecto de los cuales prestó su autorización y solicitar al responsable o al encargado informaciones sobre el uso que ha dado de sus datos personales.
3. *Principio de libertad*: el titular debe contar con la garantía de que los datos que circulen sobre él son los que él ha reconocido como susceptibles de tratamiento, solicitar prueba de su autorización e incluso revocarla.
4. *Principio de veracidad o calidad*: el titular tiene el derecho a conocer, actualizar y rectificar sus datos personales en los casos en que estos sean inexactos, incompletos o fraccionados, induzcan a error o cuyo tratamiento se encuentre prohibido. Por el principio de transparencia, el titular tiene derecho a consultar en cualquier momento el contenido exacto que de su información personal se tiene en las diferentes bases de datos, independientemente de la autorización que en un principio haya dado.
5. *Principio de acceso y circulación restringida, seguridad y confidencialidad*: los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados.

20 Ley 1581, artículo 4.

3.3 Derechos y condiciones de legalidad para el tratamiento de datos

De conformidad con lo establecido en artículo 8 de la Ley 1581 de 2012, el Titular de los datos personales tendrá los siguientes derechos:

> 1) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;
>
> 2) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;
>
> 3) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;
>
> 4) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;
>
> 5) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;
>
> 6) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Los derechos consagrados en la citada norma, y así lo ha reconocido la Corte Constitucional[21], son un desarrollo concreto de los principios rectores consagrados en el artículo 4 de la Ley 1581 de 2012.

3.3.1 La necesaria autorización del titular

Uno de los aspectos más relevantes dentro de los derechos que han sido otorgados al titular de los datos es la facultad que tiene de exigir autorización para el tratamiento de sus datos. De aquí que se diga que el derecho fundamental a la protección de datos personales tiene por objeto garantizar a toda persona el

21 Corte Constitucional, Sentencia C-748 de 2011.

poder de decisión y control que tiene sobre la información que le concierne, concretamente sobre el uso y destino que se les da a sus datos personales. En consecuencia, cada persona es dueña de su información y tiene el pleno derecho a decidir a quién y con qué finalidad proporciona sus datos personales, no estando obligada a facilitarlos si no lo desea, salvo que una ley así lo disponga.

Así, en virtud de lo establecido en el artículo 9 de la Ley 1581 de 2012, por regla general para el tratamiento de datos personales se requiere la autorización previa, consciente e informada del titular de la información. En todo caso esa autorización debe ser susceptible de ser acreditada en el futuro.

La exigencia de la autorización expresa, previa e informada del titular para la utilización de sus datos, es una expresión del principio de libertad previsto en el literal c) del artículo 4 de la Ley 1581 de 2012, de conformidad con el cual "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".

En relación con *el carácter previo*, es claro que la autorización debe ser suministrada en una etapa anterior a la incorporación del dato. Así por ejemplo, en la Sentencia T-022 de 1993 la Corte Constitucional precisó que la veracidad del dato no implica que el responsable del tratamiento no tenga el deber de obtener una autorización anterior[22]. En igual sentido, la citada corporación, mediante sentencia T-592 de 2003, dijo que "el derecho al habeas data resulta afectado cuando los administradores de la información recogen y divulgan hábitos de pago sin el consentimiento de su titular". La Corte Constitucional en la citada sentencia expresó que el consentimiento *previo* del titular de la información sobre el registro de sus datos económicos "en los procesos informáticos, aunado a la necesidad de que aquel cuente con oportunidades reales para ejercer sus facultades de rectificación y actualización durante las diversas

22 Corte Constitucional, Sentencia T-022 de 1993: "Como sujetos a quienes concierne la información, los titulares de los datos tienen los derechos que le reconocen la Constitución Política y la ley, particularmente los de acceso, certificación, rectificación y cancelación. De todo lo anterior –pero particularmente de la naturaleza misma de los datos almacenados en la Central, los cuales tienen carácter personal reconocido expresamente en el reglamento– se infiere que son idóneos para identificar a su titular y afectar eventualmente su libertad, dignidad, honor y honra. *Este riesgo –propio y característico del dato personal– explica en buena medida la exigencia de que su circulación y uso haya de estar necesariamente precedida por formal y expresa autorización de su titular, la cual, adquiere la entidad de una manifestación escrita.* Tal es, por ejemplo, el caso del reglamento de la Central de Información de la Asociación Bancaria. En estas condiciones, el titular manifiesta su consentimiento para introducir una limitación permitida por el ordenamiento a su libertad personal en desarrollo del principio de la autonomía de la voluntad. Se configura así una injerencia consentida y, como tal, no arbitraria ni abusiva en los alcances que a estos términos reconocen tanto los pactos internacionales como la doctrina" (resaltado fuera del texto).

etapas de dicho proceso, resultan esenciales para salvaguardar su derecho a la autodeterminación informática".

En relación con el *carácter expreso*, la autorización debe corresponder a una acción positiva del titular de la información. Sobre el particular, en la Sentencia C-1011 de 2008 se sostuvo que "La libertad en la administración de datos personales significa que el sujeto concernido mantenga, en todo momento, las facultades de conocimiento, actualización y rectificación de la información personal contenida en las bases de datos. Si ello es así, es evidente que la libertad del individuo ante el poder informático *se concreta, entre otros aspectos, en la posibilidad de controlar la información personal que sobre sí reposa en las bases de datos, competencia que está supeditada a que exprese su consentimiento para la incorporación de la información en el banco de datos o archivo correspondiente. Este ejercicio de la libertad en los procesos informáticos, a juicio de la Corte, se concreta en la exigencia de autorización previa, expresa y suficiente por parte del titular de la información, requisito predicable de los actos de administración de datos personales de contenido comercial y crediticio.* La eliminación del consentimiento del titular, adicionalmente, genera una desnaturalización del dato financiero, comercial y crediticio, que viola el derecho fundamental al hábeas data, en tanto restringe injustificadamente la autodeterminación del sujeto respecto de su información personal. Para la Constitución, la libertad del sujeto concernido significa que la administración de datos personales no pueda realizarse a sus espaldas, sino que debe tratarse de un proceso transparente, en que en todo momento y lugar pueda conocer en dónde está su información personal, para qué propósitos ha sido recolectada y qué mecanismos tiene a su disposición para su actualización y rectificación. La eliminación de la autorización previa, expresa y suficiente para la incorporación del dato en los archivos y bancos de datos administrados por los operadores permite, en últimas, la ejecución de actos ocultos de acopio, tratamiento y divulgación de información, operaciones del todo incompatibles con los derechos y garantías propios del hábeas data" (resaltado fuera del texto).

Bajo nuestra legislación no se admite la posibilidad de inferir la aceptación sin manifestación material alguna. En consecuencia, la autorización debe ser inequívoca y el consentimiento debe ser explícito y concreto a la finalidad específica de la base de datos.

En consecuencia, tal como lo advirtió la Corte Constitucional mediante sentencia C-748 de 2011, no está permitido el consentimiento tácito del titular del dato: "El consentimiento que brinde la persona debe ser definido como una indicación específica e informada, libremente emitida, de su acuerdo con el procesamiento de sus datos personales".

Es de resaltar el pronunciamiento de la Corte Constitucional en la sentencia T-592 de 2003, en la que se indicó que el consentimiento expreso se traducía también en la prohibición de obtener autorizaciones abiertas y no específicas. En este sentido, la corporación consideró que no obstante haberse otorgado autorizaciones para reportar la información crediticia, las mismas eran "abier-

tas y accesorias a las operaciones de crédito", por lo que no denotaban un real consentimiento de los otorgantes "en cuanto no estuvieron acompañadas de la información oportuna sobre su utilización, aparejada del alcance del reporte, ni de su contenido y tampoco del nombre y ubicación de la encargada de administrar la información". Bajo esta perspectiva reafirmada por la Corte, las autorizaciones generales o 'sombrilla'– en el sentido que todo lo cubren–, se consideran proscritas en Colombia.

Establecido lo anterior, es preciso advertir que la autorización, además de ser expresa, debe ser *informada y de la misma debe conservarse prueba*. Así, de acuerdo con lo dispuesto en literal b) del artículo 8 de la Ley 1581 de 2012, es un derecho del titular de la información solicitar la prueba de la autorización otorgada y es un deber del responsable del tratamiento conservar evidencia de dicha autorización[23] que, además de contener el consentimiento expreso del titular, deberá obtenerse en las condiciones en que lo prevé el artículo 12 de la Ley 1581 de 2012.

En efecto, el responsable del tratamiento, al momento de solicitar al titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

> 1) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
>
> 2) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
>
> 3) Los derechos que le asisten como Titular;
>
> 4) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento[24].

Establecido lo anterior, resulta importante reiterar que se deberá informar al titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y, por tanto, no podrán recopilarse datos sin la clara especificación acerca de la finalidad de los mismos. Cualquier utilización diversa, *deberá ser autorizada en forma expresa por el titular.*

Bajo la vigencia de Ley 1581 de 2012 y en desarrollo de la clara jurisprudencia de la Corte sobre las facultades y control que tiene el titular sobre sus datos personales, la autorización resulta ser la primera fuente de legitimación

23 Ley 1581 de 2012, literal b, artículo 17: "Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: "b. *Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular*" (resaltado fuera del texto).

24 Ley 1581 de 2012, artículo 12.

de cualquier operación que se realice con información que pueda ser asociada a personas identificables.

3.3.1.1. Modo de obtener la autorización

En particular frente a la manera de obtener la autorización por parte del titular, el artículo 7 del Decreto Reglamentario 1377 de 2012 dispone: "Para efectos de dar cumplimiento a lo dispuesto en el artículo 9 de la Ley 1581 de 2012, los Responsables del Tratamiento de datos personales establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 20 del presente decreto, que garanticen su consulta. Estos mecanismos podrán ser determinados a través de medios técnicos que faciliten al Titular su manifestación automatizada. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca".

En todo caso, dispone que el artículo 8 del citado decreto que el modo de obtener la autorización deberá ser adecuado para el propósito para el que se pide y deberá atender a la naturaleza de la información recolectada y que los responsables deberán conservar prueba de la autorización otorgada.

3.3.1.2. Datos recolectados antes de la expedición del Decreto Reglamentario de la Ley 1581 de 2012

Con absoluta certeza, en los últimos meses, los correos electrónicos de los colombianos se han visto plagados de mensajes enviados por diversos responsables de datos, en donde anunciaban que los datos del titular se encontraban en una determinada base de datos y se solicitaba autorización para su tratamiento. Esta práctica responde a una obligación que impuso el Decreto 1377 de 2013 para aquellos datos que hubieran sido recolectados antes de su expedición.

Al respecto, el citado decreto en su artículo 10 señaló cuáles eran los requisitos que se debían cumplir:

> 1) Los Responsables deberán solicitar la autorización de los titulares para continuar con el Tratamiento de sus datos personales (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó autorización, a través de mecanismos eficientes de comunicación, así como poner en conocimiento de estos sus políticas de Tratamiento de la información y el modo de ejercer sus derechos.
>
> 2) Para efectos de lo dispuesto en el numeral 1, se considerarán como mecanismos eficientes de comunicación aquellos que el responsable o encargado usan en el curso ordinario de su interacción con los Titulares registrados en sus bases de datos.

3) Si los mecanismos citados en el numeral 1 imponen al responsable una carga desproporcionada o es imposible solicitar a cada Titular el consentimiento para el Tratamiento de sus datos personales y poner en su conocimiento las políticas de Tratamiento de la información y el modo de ejercer sus derechos, el Responsable podrá implementar mecanismos alternos para los efectos dispuestos en el numeral 1, tales como diarios de amplia circulación nacional, diarios locales o revistas, páginas de Internet del responsable, carteles informativos, entre otros, e informar al respecto a la Superintendencia de Industria y Comercio, dentro de los cinco (5) días siguientes a su implementación.

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

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

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

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

De acuerdo con lo anterior, en principio, se advierte que para efectos de utilizar válidamente los datos personales recogidos con anterioridad a la entrada en vigencia de la Ley 1581 de 2012, es posible acudir a mecanismos técnicos eficientes que permitan obtener la autorización en forma automatizada. Es importante

precisar que el decreto admite la posibilidad de obtener la autorización, a través de los mecanismos que el responsable del tratamiento de los datos usa de manera habitual u ordinaria para relacionarse con sus respectivos clientes.

En cualquier caso, el medio técnico que se utilice deberá garantizar que se le informe al titular de los datos la manera de consultar las políticas y procedimientos para el tratamiento de la información y el modo de ejercer los derechos de acceso, consulta, actualización, rectificación y supresión de datos personales.

En el evento que la implementación de medios técnicos resulte en una carga desproporcionada, es posible disponer de mecanismos alternos, que deben ser autorizados por la Superintendencia de Industria y Comercio, por lo cual, para estos efectos, es necesario esperar a las instrucciones que imparta dicha entidad en esta materia.

3.4. Deberes de los responsables y encargados del tratamiento

Como ya habíamos precisado, el responsable del tratamiento es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos. Mientras que el encargado es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

En el artículo 17 de la Ley 1581 encontramos que los deberes de los responsables del tratamiento son:

1) Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

2) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;

3) Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;

4) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

5) Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;

6) Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;

7) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento;

8) Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;

9) Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular;

10) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

10) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;

11) Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;

12) Informar a solicitud del titular sobre el uso dado a sus datos;

13) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

14) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Los deberes de los responsables, que son en realidad quienes tienen el contacto con los titulares, buscan garantizar el pleno ejercicio del derecho al *habeas data* por parte de aquellos. Es claro que el eventual incumplimiento de alguno de estos deberes, causado por el encargado del tratamiento (en caso de ser un tercero), no resulta ser excusa suficiente[25].

25 La Corte Constitucional (Sentencia C-748 de 2011), al analizar la constitucionalidad de las reglas consagradas en el artículo 17, manifestó lo siguiente: "En relación con el *responsable del tratamiento*, es decir, aquel que define los fines y medios esenciales para el tratamiento del dato, incluidos quienes fungen como fuente y usuario, se establecen deberes que responden a los principios de la administración de datos y a los derechos –intimidad y habeas data– del titular del dato personal. "Específicamente se dispone que son deberes de esta parte de la relación:"(i) Solicitar y conservar *la autorización* para el tratamiento del dato –en los términos descritos previamente, lo que se ajusta plenamente al principio de libertad y consentimiento expreso del titular del dato. "(ii) Informar al titular la *finalidad* de esa autorización y actuar en consecuencia; por tanto, el responsable no puede conducirse por fuera de los lineamientos

De acuerdo con lo anterior, resulta claro que cualquiera que ostente la calidad de responsable del tratamiento de datos personales, tiene responsabilidades claras, concretas y precisas frente al titular del dato, y está obligado a garantizar el ejercicio pleno y efectivo del derecho al *habeas data*.

Frente a los encargados del tratamiento, la Ley 1581 en su artículo 18 consagra que sus deberes son:

> 1) Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
>
> 2) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
>
> 3) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;
>
> 4) Actualizar la información reportada por los responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;
>
> 5) Tramitar las consultas y los reclamos formulados por los titulares en los términos señalados en la presente ley;

de la autorización, lo que significa que, por ejemplo, no puede *suministrar* al encargado del tratamiento más datos que los que fueron objeto de autorización, ni puede someterlos a un tratamiento con finalidades diferentes a las informadas. En este orden de ideas, los deberes establecidos en los literales a), b) y h) son desarrollo del principio de finalidad. "(iii) Adoptar las medidas para garantizar *la seguridad del dato*, a efectos de que no se pierda, no se adultere, no se utilice o acceda por fuera de la autorización, lo cual es desarrollado en el literal d) en concordancia con el principio de seguridad en la transferencia del dato. Por tanto, el responsable está obligado a exigir y controlar las condiciones de seguridad que está empleando el encargado del tratamiento –literal a), como informar oportunamente a la autoridad encargada de la protección del dato sobre violaciones a los códigos de seguridad y la existencia de riesgos en la administración de la información de los titulares– literal n); siendo estos deberes, sin lugar a dudas, también desarrollo del principio de seguridad jurídica. "(iv)*Actualizar el dato*, hecho que lo obliga a informar oportunamente al encargado del tratamiento para hacer la actualización –literal f), deber que corresponde al principio de veracidad y calidad, como al derecho del titular del dato a actualizar toda información que sobre él se tenga en las bases de datos públicas o privadas. "(v) Rectificar e informar de forma oportuna al encargado del tratamiento sobre ese particular –literal g), para efectos de actualización. "(vi) *Tramitar las consultas y reclamos,* hecho que lo obliga a dar a conocer al encargado esas eventualidades para que éste incluya la información correspondiente en la base de datos, con anotaciones que permitan identificar fácilmente el estado de la información, es decir, para que siempre se encuentre *actualizada* –literales j) y l), e igualmente adoptar reglamentos claros para que el titular del dato pueda hacer exigible sus derechos a consultar y reclamar -literal k). "(vii) *Informar el uso* del dato al titular cuando este lo requiera –literal m), en virtud de los principios de finalidad y libertad".

6) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares;

7) Registrar en la base de datos las leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;

8) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;

9) Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;

10) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;

11) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

12) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

En conclusión, debe precisarse que los deberes enumerados en los artículos 17 y 18 de la Ley 1581 de 2012, en términos generales, buscan garantizar el pleno ejercicio del derecho al *habeas data* por parte de los titulares y en el evento en que concurran las calidades de responsable del tratamiento y encargado del tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

3.4.1. Deberes especiales

3.4.1.1. Las listas negras

Una lista negra, ordinariamente es definida como una lista de personas, instituciones u objetos que deben ser discriminados en alguna forma con respecto a los que no están en la lista. La discriminación puede ser social, técnica o de alguna otra forma[26].

26 Según el Diccionario de la RAE (2001), una lista negra consiste en la relación secreta en la que se inscriben los nombres de las personas o entidades consideradas vitandas.

Tal como lo menciona NELSON REMOLINA en la *Revista Latinoamericana de Protección de datos personales* (2013), el parágrafo 4 del artículo 14 de la Ley 1266 de 2008 ya prohibía "la administración de datos personales con información exclusivamente desfavorable". No obstante, como lo destaca el autor, desde la década de los noventa la Corte Constitucional ha rechazado este tipo de listas por las siguientes razones: "*Violan* las garantías constitucionales establecidas por el Estado Social de Derecho *porque, en ciertas ocasiones, están destinadas a* intimidar a las personas, o a amenazarles, o a hacerlas víctimas de referencias, o de las llamadas "listas negras" (T-34 de 1995)", "Son un instrumento de indebida represión, persecución o coerción contra las personas (T–761 de 2004)" y "La creación de las mismas es una práctica abusiva en la administración de datos personales porque desvirtúan la finalidad constitucionalmente legítima de los procesos de administración de datos personales" (C-1011 de 2008)".

Conforme lo relata el autor y verificando la jurisprudencia citada, el 12 de febrero de 2013 la Corte Constitucional publicó la sentencia T-987 de 2012, en la que ordenó a una empresa de transporte aéreo eliminar la base de datos denominada "lista de viajeros no conformes, destinada a la negación del acceso de servicio público esencial de transporte aéreo".

La Corte Constitucional en la citada sentencia de tutela analizó principalmente los siguientes temas: (1) Registros de información exclusivamente desfavorables (*"listas negras"* o *"blacklisting"*); (2) lista de viajeros no conformes como una herramienta ilegítima para denegar la prestación de un servicio público; (3) principios del *habeas data* como límite al tratamiento de datos personales, y (4) prácticas abusivas en la administración de datos personales.

Según lo expresa REMOLINA, "para la Corte esta práctica vulnera los derechos del debido proceso y el *habeas data*. La eliminación de esta base de datos debe hacerse de tal forma que no sea posible su consulta física o electrónica en el futuro".

A manera de sumario el autor explica que fueron varias las razones que motivaron la decisión de la Corte Constitucional:

> Incluir a un ciudadano en lo que eufemísticamente se ha denominado lista de viajeros no conformes, que no es nada distinto a un registro de denegación de servicio, carece de cualquier soporte normativo. No existe ninguna habilitación legislativa para que las compañías aéreas puedan imponer prohibiciones generales de acceso al servicio de transporte.
>
> La lista de viajeros no conformes vulnera al derecho al habeas data porque, entre otros:
>
> (i) Está prohibida la conformación de listas "de información personal con consecuencias exclusivamente desfavorables para el titular del dato, en tanto esa práctica configura un ejercicio abusivo y desproporcionado de la facultad legal de administración de datos personales";

> (ii) La inclusión de los datos personales en ese tipo de listas es contraria al principio de libertad porque no se tenía autorización del titular del dato y la empresa de servicio aéreo "hizo un uso arbitrario del permiso para la gestión de datos personales que el ciudadano… había realizado para ingresar al programa de viajero frecuente de la compañía aérea", y
>
> (iii) Desconoce el principio de finalidad y legalidad ya que su usaron datos de un ciudadano para propósitos no autorizados por el titular del dato y proscritos por la regulación.

REMOLINA argumenta que la expedición de dicha providencia genera las siguientes consecuencias:

> En primer lugar, es una sentencia con efectos "*inter comunis*" en el sentido que no solo tiene aplicación para el caso de la persona que interpuso la acción de tutela sino que favorece a todas las personas que están incluidas en la "*lista de viajeros no conformes*". Por eso la Corte ordena eliminar toda la lista de viajeros y no solo la información negativa sobre el ciudadano tutelante. En segundo lugar, la sentencia no solo obliga a la empresa de transporte aéreo directamente involucrada sino a todas las compañías aéreas que adelantan operaciones en Colombia para que "en caso que recopilen y administren información personal de sus usuarios, en las mismas condiciones y para los mismos fines en que operaba la denominada lista de viajeros no conformes que gestionaba (…), procedan a su eliminación". Para el efecto, se ordena a la Aerocivil hacer cumplir lo ordenado en la sentencia y se remite la sentencia a la Superintendencia de Industria y Comercio para que a la luz de sus competencias legales adelante las actuaciones administrativas pertinentes".

3.4.1.2 Los datos de las niñas, niños y adolescentes

De conformidad con lo establecido en el artículo 7 de la Ley 1581 de 2012, "Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública".

En relación con la citada norma, vale la pena tener en cuenta lo señalado por la Corte Constitucional que, mediante sentencia C-748 de 2011, analizó la constitucionalidad de la Ley 1581 de 2012: "Esta Sala observa que la interpretación del inciso segundo, no debe entenderse en el sentido de que existe una prohibición casi absoluta del tratamiento de los datos de los menores de 18 años, exceptuando los de naturaleza pública, pues ello, daría lugar a la negación de otros derechos superiores de esta población como el de la seguridad social en salud, interpretación ésta que no se encuentra conforme con la Constitución. *De lo que se trata entonces, es de reconocer y asegurar la plena vigencia de todos los derechos fundamentales de esta población, incluido el habeas data*. En este mismo sentido, debe interpretarse la expresión "naturaleza pública". *Es decir, el tratamiento de los datos personales de los menores de 18 años, al margen de su naturaleza,*

pueden ser objeto de tratamiento siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los niños, las niñas y adolescentes y se asegure sin excepción alguna el respeto de sus derechos prevalentes.(...) En definitiva, el inciso segundo del artículo objeto de estudio es exequible, si se interpreta que los datos de los niños, las niñas y adolescentes pueden ser objeto de tratamiento siempre y cuando no se ponga en riesgo la prevalencia de sus derechos fundamentales e inequívocamente responda a la realización del principio de su interés superior, cuya aplicación específica devendrá del análisis de cada caso en particular" (resaltado fuera del texto).

Ahora bien, a partir de las consideraciones efectuadas por la Corte Constitucional en relación con la exequibilidad del artículo 7 de la Ley 1581 de 2012, el gobierno nacional, mediante Decreto 1377 de 2013, reglamentó el tratamiento de los datos de menores de edad. Así, el artículo 12 del mencionado Decreto 1377 de 2013 establece que el tratamiento de datos personales de niños, niñas y adolecentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7 de la Ley 1581 de 2012 y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos:

1. Que se responda y respete el interés superior de los niños, niñas y adolecentes.
2. Que se asegure el respecto de sus derechos fundamentales.

Dispone el citado artículo que "Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolecente otorgará la autorización previo el ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolecentes, deberá velar por el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012 y el presente decreto. La familia y la sociedad deben velar porque los responsables y encargados del tratamiento de los datos de los menores de edad cumplan con las obligaciones establecidas en la Ley 1581 de 2012 y el presente decreto".

En virtud de las anteriores consideraciones, se advierte que es posible recoger y tratar datos de niños, niñas y adolescentes siempre que no se pongan en riesgo sus derechos fundamentales y el tratamiento obedezca al principio de su interés superior, lo que deberá analizarse en cada caso particular[27]. Se aclara

27 Corte Constitucional, Sentencia C-748 de 2011: "En definitiva, (i) el principio del interés superior de los niños, las niñas y adolescentes se realiza en el estudio de cada caso en particular y tiene por fin asegurar su desarrollo integral; (ii) este principio, además, persigue la realización efectiva de los derechos fundamentales de los menores de 18 años y también resguardarlos de los riesgos prohibidos que amenacen su desarrollo armónico. Estos riesgos

sin embargo que, previo el tratamiento de los datos personales de niños, niñas y adolecentes, se deberá contar con la respectiva autorización en los términos del artículo 8 de la Ley 1581 de 2012. La autorización para el tratamiento de los datos personales de menores de edad debe ser otorgada por su representante legal, y de ser posible, tal como lo precisó la Corte Constitucional, debe tener en cuenta la opinión del menor[28].

En conclusión, se advierte que es posible recoger y manejar datos personales de menores de edad, observando los supuestos indicados por la Corte Constitucional, y en especial, los establecidos en Decreto 1377 de 2013, que se contraen principalmente a:

1. Que el tratamiento responda y respete el interés superior de los niños, niñas y adolecentes;
2. Que se asegure el respeto de sus derechos fundamentales;
3. Que se realice teniendo en cuenta la opinión de los niños, niñas y adolecentes;
4. En el tratamiento de datos personales de niños, niñas y adolecentes deberán observarse a cabalidad los principios y obligaciones previstos en la Ley 1581 de 2012.

Resulta entonces pertinente reiterar que cuando se emplee un formulario de registro para obtener los datos del menor, es necesario eliminar la posibilidad de que personas distintas de los padres o representantes legales de los menores (quienes son los únicos facultados en principio para otorgar autorización para el tratamiento de los datos), incluyan los datos de menores de edad. Lo anterior, en la medida en que la norma expresamente establece que el representante legal del niño, niña o adolecente otorgará la respectiva autorización.

no se agotan en los que enuncia la ley sino que también deben analizarse en el estudio de cada caso particular; (iii) debe propenderse por encontrar un equilibrio entre los derechos de los padres o sus representantes legales y los de los niños, las niñas y adolescentes. Sin embargo, cuando dicha armonización no sea posible, deberán prevalecer las garantías superiores de los menores de 18 años. En otras palabras, siempre que prevalezcan los derechos de los padres, es porque se ha entendido que ésta es la mejor manera de darle aplicación al principio del interés superior de los niños, las niñas y adolescentes".

28 Corte Constitucional, Sentencia C-748 de 2011: "En definitiva, siguiendo las recomendaciones que emitió el Comité acerca de esta importante garantía, la Corte considera relevante que la opinión del menor de 18 años sea siempre tenida en cuenta, pues la madurez con que expresen sus juicios acerca de los hechos que los afectan debe analizarse caso por caso. La madurez y la autonomía no se encuentran asociadas a la edad, más bien están relacionadas con el entorno familiar, social, cultural en el cual han crecido. En este contexto, la opinión del niño, niña, y adolescente siempre debe tenerse en cuenta, y el elemento subjetivo de la norma "madurez" deberá analizarse en concreto, es decir, la capacidad que ellos tengan de entender lo que está sucediendo (el asunto que les concierne) y derivar sus posibles consecuencias".

Por lo tanto, en cualquier formulario de registro, solo se podrán incluir espacios que permitan diligenciar la información de quienes, frente al titular de la información ostenten la calidad de hijos, eliminando otro tipo de parentesco, tales como sobrinos, nietos, amigos u otros niños de la familia.

Además, debe tenerse en cuenta que es necesario adoptar especiales medidas de seguridad en las bases de datos que contengan información de niños, niñas y adolecentes que impidan su uso fraudulento o no autorizado.

4. PROCEDIMIENTOS: CONSULTAS, RECLAMOS Y AUTORIDAD COMPETENTE

De nada sirve conocer que se es titular de ciertos derechos de considerable importancia en el desarrollo de nuestra vida diaria, si no se conocen los mecanismos para hacerlos efectivos y para poder tutelarlos. De ahí que el legislador en la Ley 1581 haya previsto una serie de procedimientos para garantizar un goce pleno del derecho a la protección de los datos personales:

4.1. La consulta

La consulta, tal como lo definió la Corte Constitucional (Sentencia C-748 de 2011), es un mecanismo necesario para hacer efectivo el derecho al *habeas data*. El artículo 14 de la Ley 1581 de 2012 regula el mecanismo de la consulta al señalar al respecto lo siguiente:

> 1) Los titulares o sus causahabientes podrán consultar en todo caso la información personal del titular que repose en cualquier base de datos pública o privada.
>
> 2) Los responsables y encargados del tratamiento deben facilitar al titular que lo consulte toda la información contenida en la base de datos bien porque se tenga un registro individual o exista algún dato asociado a él.
>
> 3) El responsable y el encargado del tratamiento deben facilitar los medios para que el titular efectúe la (s) consulta (s). En todo caso ese medio debe permitir que se deje prueba de la consulta y su respuesta.
>
> 4) La consulta se debe resolver en un término máximo de 10 días hábiles a partir de la fecha de recibo de la solicitud, salvo que por razones justificadas se deba transmitir dentro de los cinco (5) días siguientes al vencimiento del primer plazo.

Definitivamente el derecho a elevar consultas, permite concretar y hacer exigible frente al responsable del tratamiento uno de los principales derechos

del titular de la información como es el de conocer la información que sobre él se ha obtenido[29].

Es un deber del responsable facilitar la formulación de estas consultas y, en la medida de lo posible, disponer de los medios para que la consulta se pueda realizar de la manera más sencilla posible.

Ahora bien, es importante tener en cuenta que al revisar la constitucionalidad del artículo 14 de la Ley 1581 de 2012, la Corte Constitucional (Sentencia C-748 de 2011) manifestó que "tanto los responsables del tratamiento como los encargados del tratamiento deben observar estos parámetros que en términos generales se pueden resumir de la siguiente manera: (i) la respuesta debe ser de fondo, es decir no puede evadirse el objeto de la petición, (ii) que de forma completa y clara se respondan a los interrogantes planteados por el solicitante y (iii) respuesta oportuna, asunto que obliga a respetar los términos fijados en la norma acusada". En este sentido, resulta de total importancia para los agremiados a Andiarios, la implementación de un procedimiento de consultas, con observancia de los términos previstos en el artículo 14 de la Ley 1581 de 2012, que permita a los titulares de la información hacer exigible su derecho a conocer la información recogida en las bases de datos o archivos. No se trata tan solo de contar con el procedimiento y elementos para absolver las consultas, estimamos de la mayor importancia que se promueva y divulgue esta importante opción con que cuentan los titulares de información.

4.2 Los reclamos

El artículo 15 de la Ley 1581 de 2012 regula el procedimiento de reclamos cuyo objeto es obtener la corrección, actualización o supresión de datos personales, o cuando se considere que se ha incumplido con cualquiera de los deberes previstos en los artículos 17 y 18 de la ley.

El artículo 15 fija las reglas que deben observar los responsables del tratamiento de los datos para tramitar los reclamos, en los siguientes términos:

> 1) El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo. En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

29 Ley 1581 de 2012, artículo 8 literal a.

> 2) Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.
>
> 3) El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

En cuanto al trámite, además de la estricta observancia de los términos para resolver la reclamación, es importante tener en cuenta que una vez el responsable se entera de la existencia del reclamo, debe acompañar al registro de la información la expresión "reclamo en trámite", haciendo referencia al motivo del mismo. Esta anotación permanecerá en el registro hasta que el reclamo se defina. Lo anterior, con independencia de la naturaleza del reclamo o lo fundado o infundado que en un primer momento pueda parecer.

Es importante llamar la atención sobre el hecho que la implementación de procedimiento de reclamos es una obligación legal a cargo del responsable del tratamiento de los datos y constituye un "mecanismo le permitirá al titular del dato o a sus causahabientes solicitar al encargado o responsable del tratamiento, el cumplimiento de todos los principios que rigen a los administradores de datos y los derechos del titular del dato, razón por la que no considera necesario condicionar el precepto en revisión en el sentido en que lo solicita esa entidad, por cuanto si bien la norma sólo se refiere a la actualización, corrección o supresión, no significa que no se puedan solicitar otras dimensiones de este derecho si a ello hay lugar"[30].

De otra parte, se observa que el procedimiento de reclamos constituye una oportunidad que permite a los responsables del tratamiento resolver de manera directa las inconformidades planteadas por los titulares de la información en relación con el manejo de sus datos, evitando de esta manera que tales reclamaciones lleguen a la Superintendencia de Industria y Comercio donde eventuamente se podrían iniciar procedimientos administrativos de tipo sancionatorio.

4.3 La autoridad competente

Lo primero que hay que determinar es si se está en presencia de información financiera, crediticia, comercial, de servicios o proveniente de terceros países de la misma naturaleza y si la fuente, usuario u operador de esa información

30 Corte Constitucional, Sentencia C-748 de 2011.

es una entidad vigilada por la Superintendencia Financiera de Colombia. Si ambas respuestas son afirmativas, la vigilancia, inspección y eventual sanción estarán a cargo de la Superintendencia Financiera, tal y como lo dispone la Ley 1266 de 2008.

En los demás casos, dispone la Ley 1581 que la autoridad en materia de protección de datos será la Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales.

En concordancia con lo dispuesto en los artículos 16 y 17 del Decreto 4886 de 2011, "Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones", el artículo 21 de la Ley 1581 señala como funciones de la Delegatura para la Protección de Datos Personales, las siguientes:

> 1) Velar por el cumplimiento de la legislación en materia de protección de datos personales;
>
> 2) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;
>
> 3) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva;
>
> 4) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementará campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos;
>
> 5) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley;
>
> 6) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones;
>
> 7) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos;
>
> 8) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento;

> 9) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional;
>
> 10) Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personajes;
>
> 11) Las demás que le sean asignadas por ley.

Resulta importante señalar que el artículo 16 de la Ley 1581 de 2012 establece un requisito de procedibilidad para la interposición de quejas ante la Superintendencia de Industria y Comercio. En efecto, el titular o causahabiente solo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado los trámites de consulta o reclamo, explicados antes, ante el responsable del tratamiento.

Se advierte además que el artículo 22 de la Ley 1581 de 2012 remite al Código Contencioso Administrativo en relación con el procedimiento aplicable para la imposición de las sanciones que a continuación se explican, por lo cual la Superintendencia de Industria y Comercio deberá observar las reglas contenidas en la parte primera de la Ley 1437 de 2011 –Código Contencioso Administrativo–.

El artículo 23 de la Ley 1581 de 2012 establece las sanciones que puede aplicar la Superintendencia de Industria y Comercio a los responsables del tratamiento y encargados del tratamiento por la infracción de cualquiera de las disposiciones de la ley, dentro de las cuales contempla las multas–hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes–, la suspensión de las actividades relacionadas con el tratamiento, el cierre temporal de las operaciones relacionadas con el tratamiento y finalmente el cierre inmediato y definitivo de la operación.

En lo que tiene que ver con la dosimetría de la multa, el artículo 24 de la citada ley señala una serie de criterios para determinar la sanción aplicable. Estos son: "a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley. b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción. c) La reincidencia en la comisión de la infracción. d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio. e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio. f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar".

De acuerdo con lo anterior, es claro que la infracción de las disposiciones contenidas en la Ley 1581 de 2012, en especial el incumplimiento de los deberes previstos en los artículos 17 y 18 para los responsables y encargados del

tratamiento, puede dar lugar la imposición de las sanciones arriba señaladas cuya graduación efectuará la Superintendencia de Industria y Comercio, de conformidad con los parámetros del artículo 24, dependiendo de factores o circunstancias del investigado o de su actuación.

5. IMPLEMENTACIÓN DE OBLIGACIONES POR PARTE DE LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO

La implementación de las obligaciones, y en general de todas las disposiciones contenidas en la ley de protección de datos personales debió realizarse dentro del plazo previsto en el artículo 18 de la ley, esto es, dentro de los seis (6) meses contados a partir de su entrada en vigencia. Dicho plazo venció el pasado *18 de abril de 2013* y, por lo tanto, resulta de suma importancia que todos los usuarios procuren la verificación del cumplimiento de lo allí exigido y de notar alguna discordancia o presentar alguna inconformidad con el tratamiento que se les está dando a sus datos, agotados los procedimientos en sede de responsable o encargado, acuda ante la autoridad competente, bien sea la Superintendencia Financiera o la Superintendencia de Industria y Comercio.

BIBLIOGRAFÍA

Constitución Política de 1991.

Corte Constitucional Sentencia T-444 de 1992.

Corte Constitucional, Sentencia T-022 de 1993.

Corte Constitucional Sentencia T-580 de 1995.

Corte Constitucional Sentencia SU-082 de 1995.

Corte Constitucional Sentencia T-448 de 2004.

Corte Constitucional Sentencia T-526 de 2004.

Corte Constitucional Sentencia T-657 de 2005.

Corte Constitucional Sentencia T-684 de 2006.

Corte Constitucional, Sentencia C-1011 de 2008.

Corte Constitucional Sentencia C-1011 de 2008.

Corte Constitucional, Sentencia T-729 de 2009.

Corte Constitucional Sentencia C-748 de 2011.

Corte Constitucional Sentencia T-017 de 2011.

Corte Constitucional, Sentencia C-748 de 2011.

Corte Constitucional, Sentencia C-748 de 2011.

Corte Constitucional, Sentencia C-748 de 2011.

Corte Constitucional, Sentencia T- 260 de 2012.

Decreto 1377 de 2013.

Ley 1266 de 2008.

Ley 1581 de 2012.

Organización de las Naciones Unidas (1990). Resolución 45/95 sobre los principios rectores sobre la reglamentación de los ficheros computarizados de datos personales. 14 de diciembre de 1990. Disponible en http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/572/58/IMG/NR057258.pdf?OpenElement.

Organization por Economic Cooperation and Development (1980). *Guidelines on the protection of privacy an transborder flows of personal data*. Disponible en http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

RAE (2001). Diccionario de la Lengua Española. Edición 22ª. Disponible en www.rae.es.

Remolina, Nelson (2013). "La Corte Constitucional Colombiana reitera su rechazo al uso de las 'listas negras'", en *Revista Latinoamericana de Protección de Datos Personales*. Marzo 31 de 2013. Disponible en http://www.rlpdp.com/2013/03/nelson-remolina-la-corte-constitucional-colombiana-reitera-su-rechazo-al-uso-de-las-listas-negras/.

Unión Europea - Parlamento Europeo y el Consejo de la Unión Europea (1995). Directiva 95/46 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. 24 de octubre de 1995. Disponible en http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML.