Clasificación de los datos personales e implicaciones legales

Natalia Hernández Lotero

Universidad Pontifica Bolivariana

Nota del autor

Estudiante de Derecho en la Universidad Pontificia Bolivariana.

Artículo elaborado para optar al título de abogada, en el marco de la práctica corporativa, dirigido por el docente Doctor en Derecho: Néstor R. Londoño S.

Más información sobre este artículo en: natyhelo_1989hotmail.com

Resumen

El presente artículo explica los datos personales en Colombia, como se encuentran clasificados y las consecuencias legales al incumplimiento de la normatividad, que es de gran importancia en la actualidad, donde se hace un recuento de los antecedentes normativos que dieron surgimiento a este tema, investigación que parte desde la legislación colombiana y condice hasta el derecho internacional.

La protección de datos personales en Colombia surge con dos sistemas normativos, la ley 1266 de 2008 referente al Habeas data financiero, crediticio y comercial y con la ley 1581 de 2012 referente a cualquier dato personal almacenado en bases de datos de entidades públicas y privadas básicamente.

La ley 1266 de 2008 define las clases de datos de carácter personal, como dato privado, dato semiprivado y dato público. Adicionalmente, la Ley 1581 de 2012 establece unas categorías especiales de datos personales, como lo son los datos sensibles y lo datos personales de los niños, niñas y adolescente.

Por último, en este artículo se pretende no solo poner en conocimiento la normatividad en protección de datos personales, sino también permitir que las entidades públicas y privadas determinen la manera cómo debe ser tratados estos datos según su clasificación, teniendo presente que es indispensable la autorización para el tratamiento de datos en los casos señalados por la ley.

Palabras claves

Protección de datos, Derecho a la privacidad, Derecho de la informática.

Introducción

El tema a abordar en este artículo parte de la clasificación de los datos personales, su significado y las consecuencias legales, tema que se encuentra en contexto con la ley 1581 de 2012 referente a la protección de datos personales. El artículo se realizó con la intención de profundizar sobre un tema que, aunque no es nuevo en la normatividad vigente, si es aún desconocido por personas naturales y jurídicas en el ejercicio del comercio o cualquier actividad que implique almacenamiento de información sobre personas naturales en bases de datos, para poder lograr concientizarlas del verdadero uso que se le está dando a los datos personales y así evitar las posibles sanciones legales que trae el desconocimiento de esta información o el incumplimiento de la normatividad.

Seguramente a muchas personas les ha pasado que de manera imprevista son sorprendidos por llamadas de algunas empresas ofreciéndoles algún producto o información y que quizás esta persona siente invadida su privacidad porque nunca ha suministrado su información personal o ha autorizado su uso y esto es así, porque el almacenamiento y tratamiento de datos personales es más común por parte de las empresas dedicadas al comercio entendiendo que para ellos es fundamental esta actividad para poder desarrollar su objeto social, como por ejemplo el envío de información promocionando productos a sus clientes, solicitudes a sus proveedores, compartir información privada de sus empleados con otras entidades, entre otras actividades, que aunque cada empresa las maneja de manera diferente, requieren de un mismo medio y es el tratamiento de datos personales.

Por esta razón, es trascendental hablar sobre la clasificación de los datos personales en Colombia para entender el riesgo que se corre y la importancia de protegerlos.

Este articulo tiene relación directa con la práctica realizada porque consistía en apoyar las labores del oficial de protección de datos, quien es el responsable de las bases de datos de las empresas, es un cargo o rol nuevo en el ámbito empresarial exigido por el Ministerio de Industria y Comercio y en compañía de ese oficial se llevaban a cabo labores como recolección de autorizaciones para el tratamiento de datos de empleados, clientes y proveedores, se capacitaba al personal sobre la existencia e importancia de la Ley 1581 de 2012, ya que eran ellos quienes tenían contacto directo con el cliente y quienes recolectaban cualquier tipo de información que podía ser concebida como un dato personal.

Igualmente dentro de las actividades del oficial estaba realizar auditorías internas para velar por el cumplimiento de la normatividad cuando se almacenaban datos personales y se elaboraban los respectivos contratos de transmisión de datos personales cuando se compartía información de clientes y proveedores a otras entidades o personas naturales, entre otras funciones; es allí entonces, donde realmente se evidenciaron las operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión, y donde además fue fundamental el conocimiento de la clasificación de los datos personales para lograr una correcta implementación de la ley.

Este tema es de gran importancia porque permite proteger la privacidad de los clientes, conocer y comprender la norma y evitar posibles sanciones y multas establecidas por la ley que pueden llegar hasta los 2.000 salarios mensuales legales vigentes.

1. Los datos personales en Colombia y sus antecedentes

Debido a la creciente existencia y uso de las telecomunicaciones y la tecnología ha sucedido que en la mayoría de las ocasiones los datos personales han sido utilizados con finalidades distintas con las que verdaderamente fueron recaudadas o suministradas y al presentarse esta situación se está atentando contra la privacidad del titular de esos datos.

Es por esto que surgió la necesidad de crear un sistema de protección a la vulneración de este derecho a la intimidad y privacidad, por tal motivo nació en Europa el concepto de "protección a los datos personales" con la llamada "ley del censo" que luego de entrar en vigencia desato una protesta en Alemania, ya que el Estado pretendía una operación censal en la que se exigía al ciudadano una información personal casi absoluta teniendo como consecuencia la vulneración de los derechos protegidos en la Ley fundamental de Bonn de 1949, como el derecho a la dignidad humana y al libre desarrollo de la personalidad.

Debido a lo anterior el Tribunal Constitucional Alemán suspendió dicha ley por considerar tal vulneración de los derechos anteriormente mencionados, garantizando la libertad con la formación de un derecho nuevo, el derecho a la "autodeterminación informativa" esto es, que toda persona pueda ejercer control o pueda decidir libremente sobre la información personal que desee o le interese compartir. Este nuevo derecho surgió con la sentencia expedida por el Tribunal Constitucional Alemán el 15 de diciembre de 1983.

De igual manera existen otras fuentes internacionales como la "Declaración Universal de Derechos Humanos", que en su artículo 12 se señala que "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su*

honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias."

Así mismo, con el "derecho a la intimidad" consagrado en el "Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales" en su artículo 8 , en la "Convención Americana de Derechos Humanos (Pacto de San José)" en su artículo 11, entre otras legislaciones nace la protección a los datos personales.

En Colombia, gracias a estos antecedentes normativos y fuentes internacionales, se empieza a adoptar un sistema de protección al derecho a la intimidad con la Constitución Política de 1991 en sus siguientes artículos:

> *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 los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (Constitución Política de Colombia de 1991, artículo 15).*
>
> *Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad (Constitución Política de Colombia de 1991, artículo 20).*

De igual manera en materia de protección de datos personales, existen dos regulaciones sobre el tema, la primera de ellas es la Ley 1266 del 2008, que hacía énfasis exclusivamente en la protección de datos de carácter financiero y comercial, reportados en las centrales de riesgo, expresado en el objeto de la ley:

> *Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países (Ley habeas data, 2008).*

Con posterioridad a la anterior normatividad, se creó la Ley Estatutaria 1581 de 2012 que fue reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y que rige actualmente aplicable a todas las bases de datos de entidades públicas y privadas que almacenen y utilicen datos personales de manera general, así como lo indica la Ley en su objeto:

> *Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma (Ley de protección de datos personales, 2012).*

Sin embargo, esta Ley no es aplicable a las bases de datos almacenadas de manera doméstica, las de seguridad nacional, las de inteligencia, contrainteligencia, las de contenido

periodístico y de censos, así como las reguladas por la Ley 1266 de 2008, mencionada anteriormente.

En cuanto a los antecedentes jurisprudenciales en Colombia , encontramos la Sentencia T-414 de 1992 en su apartado que dice "*Se protege la intimidad como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad*" además, considera la Corte en la sentencia , que toda persona por el hecho de existir tiene derecho a la intimidad y que es la persona misma la responsable y la autorizada de divulgar sus datos privados. También encontramos la Sentencia T-444 de 1992 en donde expresa que el habeas data, es el derecho que implica poder exigir el conocimiento de los datos que se tengan almacenados de nosotros mismos y la posibilidad de solicitar su corrección, con el fin de proteger la intimidad debido al tratamiento que las diferentes entidades hacen a los datos de las personas, agregando la Corte en este apartado:

> *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.*

Podemos encontrar otras sentencias de la Corte Constitucional sobre protección de datos personales como lo son, Sentencia SU-082/95, Sentencia T-814/03, Sentencia C-1011/08, entre otras.

Clasificación de los datos personales

Es importante comenzar definiendo el concepto de "Dato" proveniente del latín "*datum"* que significa "lo que se da" es decir, un dato es toda información que se brinda, de manera alfabética, numérica, es una representación simbólica sobre hechos, elementos, etc. Ahora bien, Cuando se habla de un dato personal se hace alusión a la información que permite individualizar e identificar a una persona como por ejemplo, su nombre, número de identificación, edad, número telefónico, información de salud, correo electrónico, dirección de residencia, información financiera, orientación sexual, política y religiosa, etc.

La Corte Constitucional en la sentencia C-748 de 2011 señala las características de los datos personales:

> *i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente*

> *en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación.*

Hoy en día en Colombia, estos datos son almacenados de diversas maneras, como por ejemplo de forma "no automatizada", esto es, datos que se encuentren almacenados en medios físicos, como archivos, fichas de pedido de proveedores, hojas de vida físicas, un cuaderno, etc. O también de manera "automatizada", es decir almacenada en medios informáticos o virtuales, bien sea por personas naturales o jurídicas, públicas o privadas.

Debido a las diferentes formas en que son almacenados los datos personales es que surge la importancia de clasificarlos y darles una categoría a cada uno ya que según el tipo de dato será el grado de protección, es por ello que la Ley es clara en garantizar esa protección y lo que pretende es establecerle a los responsables del almacenamiento, es decir, las entidades públicas o privadas, personas naturales o empresas comerciales, exigiéndoles unas medidas de seguridad dependiendo del tipo de dato del que se trate, esto con la finalidad de evitar posibles sanciones.

La Ley 1266 de 2008 trae una categorización de los datos personales, clasificándolos en "datos privados" "datos semiprivados" y "datos públicos", además, la Ley 1581 de 2012 consagra unas categorías especiales de los datos personales, denominándolos "Datos sensibles" y "Datos personales de los niños, niñas y adolescentes", entonces, actualmente los datos en Colombia se clasifican en, "datos personales" "datos públicos" "datos privados" dato semiprivados", "datos sensibles" y " datos de niños, niñas y adolecentes".

Dato público

Son aquellos datos personales que las normas y la Constitución han determinado expresamente como públicos y los que no sean semiprivados, privados o sensibles y para cuya recolección y tratamiento no es necesaria la autorización del titular de la información, son datos públicos, por ejemplo, lo relativo al estado civil de las personas, su nombre, su número de identificación, fecha de nacimiento, lo relativo a su profesión u oficio y a su calidad de comerciante o servidor público, entre otros. Por su naturaleza, los datos públicos pueden estar contenidos, en registros públicos, documentos públicos, gacetas y boletines oficiales o en sentencias judiciales ejecutoriadas que no estén sometidas a reserva.

A pesar de no ser necesaria la autorización del titular para su uso, se deberá en todo caso cumplir con las disposiciones de la Ley 1581 de 2012 y sus decretos reglamentarios, en especial la aplicación de los principios para el tratamiento de los datos personales, como lo son, el principio de legalidad, finalidad, seguridad, necesidad, principio de acceso y circulación restringida, confidencialidad, entre otros, consagrados en el artículo 4 de la misma ley.

Es importante hacer una salvedad, ya que el dato público no es tan público como se cree, pues si bien es cierto que es un dato de amplia circulación para todo el mundo, la Superintendencia ha considerado unas limitantes para este criterio de clasificación, como lo expresa en la Resolución 15339 del 2016, donde por ejemplo manifiesta, que un dato personal no va a tener la naturaleza de dato público por el simple hecho de que se encuentre en una fuente de acceso público, como por ejemplo, en redes sociales, publicación en medios de comunicación, páginas de internet, etc. Esto significa que aunque estén allí publicados, no pierden su naturaleza de datos privados, sensibles o semiprivados por el hecho de acceder fácilmente a ellos para una consulta. Entendiéndose entonces, que si accedo a estos datos personales que se encuentran almacenados de manera pública

para otra finalidad distinta a la de mera consulta, como por ejemplo para enviar publicidad de productos y servicios, seria indispensable la autorización para su tratamiento.

Así mismo, en un concepto emitido por la Superintendencia de Industria y Comercio, donde se expresa que cuando se pretenda, por ejemplo, tratar información pública que este en internet, debe someterse al cumplimiento del principio de finalidad de la base de datos.

Si bien es cierto que la definición de dato público contiene la expresión "*los que no tengan la naturaleza de semiprivado, privado o sensible.*" Sobre esto se pronunció la Corte Constitucional en la sentencia C- 1011 de 2008, donde analiza algunos aspectos puestos a consideración por los intervinientes y el Procurador General, relacionados con la exequibilidad de una "presunción de dato público" y la delimitación del concepto de "interés". Esta definición, a juicio de los intervinientes y del Ministerio Publico, atentaría contra el derecho a la intimidad, ya que esto permitiría una interpretación libre o arbitraria de lo que realmente puede significar una información personal a la condición de dato público.

Con respecto a lo anterior, la Corte considera que, aunque esa definición puede generar confusión, realmente su interpretación se debe dar desde la definición de un dato privado y semiprivado, que perfectamente se distinguen del dato público en razón al mayor o menor grado de interés. Así las cosas, la Corte concluye que esa expresión "*todos aquellos que no sean privados o semiprivados*" es insignificante o innecesaria, porque la misma norma se encarga de establecer que datos se adecuan a esas categorías, debido a esto no resulta posible sostener una interpretación que permita que un dato personal vinculado al contenido y alcance del derecho a la intimidad resulte incorporado al concepto de dato público, pues es lógico que por sus características particulares se ubicaría bien en la categoría de dato semiprivado o de dato privado.

Dato semiprivado

La ley 1266 de 2008 trae la definición en su artículo 3 literal g):

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 se refiere el Título IV de esta ley.

La Corte Constitucional precisa en la Sentencia C-1011 de 2008 que los datos semiprivados, por tratarse de información personal o impersonal y no encajar en la definición de dato público, para su acceso, tratamiento o divulgación tiene una limitante y es que requiere orden de autoridad administrativa o judicial y que sea para los fines propios de sus funciones, como por ejemplo, historias crediticias, datos financieros, reporte en las centrales de riesgo, precisando que este tipo de datos requieren de autorización previa del titular para ser reportados a las bases de datos, o centrales de riesgos.

Dato Privado

Según la definición de la Ley 1266 de 2008 "*Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular*" esto significa que un dato privado es cualquier información que se refiere a la vida privada de una persona como lo son sus datos personales, tales como, correo electrónico personal, teléfono, dirección de vivienda, datos laborales, nivel de escolaridad, sobre infracciones administrativas o penales, los datos administrados por algunas entidades como tributarias, financieras o de la seguridad social, fotografías, videos, y cualquier

otro dato que referencien el estilo de vida de la persona. Dicha información no debe ser observada o tener acceso indebido por ningún órgano público o privado, ya que el titular tiene derecho a controlar cuando y quien puede acceder a esa información que hace parte de su vida privada. Además, cabe mencionar que:

> *Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la ley 1581 de 2012 (Sentencia C- 748 de 2011).*

Por tal motivo, es importante manifestar que se encuentra prohibida la obtención y divulgación de los datos personales sin la previa autorización del titular o en ausencia de mandato legal o judicial, autorización que debe ser además expresa e informada. La sentencia SU-082 de 1995, afirmó: "*los datos conseguidos, por ejemplo, por medios ilícitos no pueden hacer parte de los bancos de datos y tampoco pueden circular*." En el mismo sentido, en la Sentencia T-176 de 1995, se consideró como una de las hipótesis de la vulneración del derecho al habeas data el de la recolección de la información "*de manera ilegal, sin el consentimiento del titular de dato*".

Dato sensible

Es una categoría especial de datos de carácter personal especialmente protegido por la Ley 1581 de 2012, se refiere a todos aquellos datos que se relacionan con el nivel más íntimo de la persona y cuyo uso indebido puede generar su discriminación. No puede ser objeto de tratamiento

a menos que sea requerido para salvaguardar un interés vital del titular o este se encuentre incapacitado y su obtención haya sido autorizada expresamente.

De manera general, se consideran datos sensibles aquellos que revelan características como origen étnico o racial, datos de salud, preferencia sexual, filiación política, religión, ideología, afiliación a sindicatos, organizaciones sociales, datos biométricos, entre otros. Es por esto que esta clase de información debe ser tratada con mayor responsabilidad.

La Ley 1581 de 2012 prohíbe el tratamiento de datos sensibles con excepción de los siguientes casos:

> *(i) cuando el Titular otorga su consentimiento, (ii) el Tratamiento es necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado, (iii) el tratamiento es efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad, (iv) el Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y (v) el Tratamiento tenga una finalidad histórica, estadística o científica, en este último caso deben adoptarse las medidas conducentes a la supresión de identidad de los Titulares.*

Dato biométrico. Este es un tipo de dato sensible que amerita una explicación adicional. La biometría hace referencia a las tecnologías que miden y analizan los parámetros y características del cuerpo humano, parámetros físicos que son únicos en cada persona para poder comprobar su identidad como lo son las huellas dactilares o el iris del ojo, fotografías, cámaras de video vigilancia, placas dentales, aunque los científicos también son capaces de identificar a un individuo por su voz, su palma de la mano o rasgos del rostro. Esto viene regulado por España en su Ley Orgánica de Protección de Datos (LOPD) de 1999, la cual define en su artículo 3 como "*cualquier información concerniente a personas físicas identificadas o identificables*"**.**

Los datos biométricos se utilizan actualmente en los campos de la seguridad y la medicina y se usan para permitir el acceso a edificios o a zonas muy restringidas sin necesidad de utilizar tarjetas o claves de acceso que pueden transferirse fácilmente de una persona a otra. En Colombia, por ejemplo, nos piden la huella dactilar para casi todo, nos toman fotos en cualquier parte y nos "videovigilan" permanentemente, también podemos ver claramente cuando algunos dispositivos móviles requieren de huella dactilar para poder acceder a ellos, es por esto por lo que también se consideran datos sensibles ya que la información contenida está ligada directamente con la intimidad de la persona y por ello la importancia de protegerlos.

Datos de niños, niñas y adolescentes

En cuanto a los datos personales de los niños, niñas y adolescentes se debe tener en cuenta que la ley 1581 de 2012 prohíbe su tratamiento, salvo aquellos que por su naturaleza son públicos. Sin embargo, la Corte Constitucional manifestó que sin importar la naturaleza de los datos, se puede dar el tratamiento de los mismos "*siempre y cuando el fin que se persiga con dicho tratamiento*

responda al interés superior de los niños, niñas y adolescentes y se asegure sin excepción alguna el respeto a sus derechos prevalentes".

Implicaciones legales

Es importante que las entidades públicas y privadas tengan claros los criterios de clasificación de los datos personales y que el tratamiento que hagan de los datos de cualquier titular siempre sea conforme a lo expresado por la normatividad vigente en protección de datos personales , ya que su uso indebido puede generar implicaciones legales que serán impuestas por la Superintendencia de Industria y Comercio, como sanciones que van desde multas , cese de actividades comerciales hasta cierre de la entidad o empresa, de igual manera estas sanciones serán generadas de acuerdo al grado de incumplimiento, es decir, a mayor violación de la intimidad mayor será la sanción, como por ejemplo, un colegio que vulnere los derechos fundamentales de un menor de edad divulgando información del mismo sin la autorización expresa consagrada en la ley incurrirá en una sanción económica bastante grande a comparación de una entidad dedicada al comercio que hace uso indebido de un dato personal de un titular, que en este caso podría ser menor la sanción. En conclusión, dependiendo de dónde se ubique el dato vulnerado es decir, si es privado, publico, sensible o semiprivado será el grado de sanción.

La Superintendencia de Industria y Comercio en el ejercicio de sus funciones de vigilancia, control e inspección ha impuesto 619 multas desde el año 2010, que supera casi los $20.000 millones de pesos, pero los incumplimientos comunes son las violaciones del habeas data financiero en la ley 1266 de 2008. Algunas de las faltas cometidas son por ejemplo la utilización de información de personas con fines de mercadeo sin la autorización del titular, las fallas en la seguridad de la información que dan lugar a la divulgación de los datos en Internet, incluso de datos sensibles, el hurto y/o pérdida de la información contenida en bases de datos, no comunicarle al deudor que será reportado en una central de riesgo antes de hacerlo, haber reportado ante las

centrales de riesgo información del titular que no comprende con la realidad , como por ejemplo que no es deudor, entre otros.

Sin embargo, hoy en día, existen muchas entidades donde los responsables o encargados aún desconocen la ley 1581 de 2012 e incurren en gravísimas faltas por no darle su cumplimiento, es por esto que la ley trae en su artículo 23 las sanciones:

> *La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:*
>
> *a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;*
>
> *b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;*
>
> *c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;*
>
> *d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;*
>
> *Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad*

pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

Veamos algunos de los casos de incumplimiento de la ley de protección de datos personales y las sanciones correspondientes.

Acto administrativo 27708 de 2017, por el cual se impone una sanción a la sociedad Ripley Compañía de Financiamiento S.A y al Centro Comercial Oviedo PH por la presunta violación de las normas de protección de datos personales contenidas en la ley 1581 de 2012, donde la sociedad Ripley le hace envío de correos electrónicos y mensajes de texto a una persona promocionando una tarjeta de crédito y una rifa de un vehículo, el señor molesto por estos envíos publicitarios presenta queja ante la Superintendencia de Industria y Comercio.

Por tal situación se abre investigación a Ripley y al centro comercial Oviedo, pero se logra probar que el centro comercial celebró un acuerdo verbal con la sociedad Ripley para una publicidad donde Oviedo le compartió su base de datos de los clientes, actuando éste como responsable del tratamiento de los datos personales. Es Oviedo también responsable de violar las normas de protección de datos personales porque cuando recolectó los datos de la persona no logró probar ante la Superintendencia de Industria y Comercio la autorización expresa e informada del titular que en este caso eran datos privados como su número de teléfono y correo electrónico, se dio lugar entonces a una sanción que comprendió una multa de 30 smlmv por haber violado lo dispuesto en el artículo 17 de la ley 1581 de 2012.

Otro caso más complejo y de mayor grado de sanción fue a Colmedica Medicina Prepagada S.A., porque divulgo datos personales, semiprivados, privados, de naturaleza sensible y algunos relativos a niños, niñas y adolescentes de 30 de sus usuarios en el portal de internet, donde

cualquier persona tenía acceso libremente y podía ver información sensible de algunos de ellos como exámenes médicos, historias clínicas, entre otros, con una multa de $827.346.000 millones de pesos lo que equivale a 1200 salarios mínimo mensuales legales vigentes en Colombia, y es ahí donde vemos que la multa se impone de manera proporcional, esto es, de acuerdo al daño causado es que se evalúa el monto de la multa, y en este caso como se trata de datos sensibles que tocan con la intimidad de la persona es por ello que el valor es mucho mayor al primer caso. Acto administrativo 39398 del 2016.

Conclusiones:

Es importante que antes de implementar la ley 1581 de 2012 en cualquier entidad pública o privada se tenga muy claro las categorías que trae la misma ley en cuanto a las bases de datos ya que esto permite una mejor organización tanto interna como externa, adquiere mayor confianza en los mismos clientes o titulares y permite una protección jurídica de malas prácticas, garantizando estándares de seguridad informática para evitar posibles sanciones por el incumplimiento de la misma ley.

Los datos personales en Colombia se clasifican en datos privados, semiprivados, público y sensibles, incluyendo en este último grupo los de niños niñas y adolescentes y los datos biométricos que hoy en día son de amplia utilización para la seguridad, recordando que los datos deben siempre ser categorizados para ser tratados conforme la ley, esto es, cada que recolectemos datos de un titular es importante tener claro a qué grupo de datos pertenece para poder darle el tratamiento adecuado, para esto se hace indispensable contar siempre con la autorización expresa por pate del titular para poder utilizar, transferir y en general tratar los datos, en los casos que la ley lo requiera.

Referencias

Alemania. *Ley Fundamental para la República Federal de Alemania.* (1949)

Alemania. Tribunal Constitucional Alemán. *Ley del censo,* (1983).

Asamblea General de las Naciones Unidas (1948). *Declaración universal de los derechos humanos*.

Colombia. Congreso de la Republica de Colombia. *Ley de Habeas Data* 1266 (2008)

Colombia. Congreso de la Republica de Colombia. *Ley Estatutaria de Protección de Datos Personales 1581* (2012)

Colombia. Constitución política de Colombia. (1991)

Convención Americana Sobre Derechos Humanos, 11. (1969).

Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, 8. (1950)

Corte Constitucional (1992). Bogotá. Sentencia T-414. Magistrado Ponente: Ciro Angarita Barón.

Corte Constitucional (1992). Bogotá. Sentencia T-444. Magistrado Ponente: Alejandro Martínez Caballero.

Corte Constitucional (1995). Bogotá. Sentencia No. SU-082. Magistrado Ponente: José Gregorio Hernández Galindo.

Corte Constitucional (1995). Bogotá. Sentencia T-176. Magistrado Ponente: Eduardo Cifuentes Muñoz

Corte Constitucional (2003). Bogotá. Sentencia T-814. Magistrado Ponente: Rodrigo Escobar Gil.

Corte Constitucional (2008). Bogotá. Sentencia C-1011. Magistrado Ponente: Jaime Córdoba Triviño.

Corte Constitucional (2011). Bogotá. Sentencia C-748. Magistrado Ponente: María Victoria Calle Correa.

España. *Ley orgánica de protección de datos*. (1999)

Pérez Porto, J., & Merino, M. (2009). Definición de datos. Obtenido de definicion.de: https://definicion.de/datos/

Rojas Bejarano, Marcela. (2014, Enero). *Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales (*Artículo, Universidad Católica de Colombia, Bogotá, Colombia) Recuperada de: http://editorial.ucatolica.edu.co/ojsucatolica/revistas_ucatolica/index.php/Juridica/article/viewFile/652/670

Superintendencia de industria y comercio. *Acto administrativo 27708* (2017)

Superintendencia de industria y comercio. *Acto administrativo 39398* (2016)

Superintendencia de industria y comercio. *Resolución 15339* (2016)