INFRACCIONES A LA LEY DE PROTECCIÓN DE DATOS PERSONALES (LEY 1581 DE 2012) EN LOS PROCEDIMIENTOS SANCIONATORIOS TRAMITADOS POR LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO ENTRE LOS AÑOS 2020 Y 2022.[1]

Andrés Felipe Marín Ospina[2]

RESUMEN

Si de recursos valiosos se trata, para las entidades con ánimo comercial principalmente, la información personal de su público objetivo es uno de los más importantes. Por esto, es que la mayoría de empresas ahora están enfocadas en contar con bases de datos robustas, mismas que pueden ser supremamente valiosas usadas de la mano con el desarrollo tecnológico que tenemos actualmente. Sin embargo, la recolección y uso de esta información, cuenta con una regulación legal en Colombia para evitar que se vulneren derechos fundamentales de los ciudadanos, como lo es la intimidad, el libre desarrollo de la personalidad, el buen nombre, etc. Se presenta entonces un artículo dentro del cual se exponen los hallazgos arrojados por una investigación en donde se analizaron los procedimientos sancionatorios adelantados por la Superintendencia de Industria y Comercio (en adelante SIC) entre los años 2020 y 2022 buscando identificar cuáles son las faltas más recurrentes a la norma, que finalmente, tienen como consecuencia una sanción impuesta por este ente de vigilancia y control.

PALABRAS CLAVE

Dato personal, tratamiento de datos, derecho fundamental, datos públicos, datos semiprivados, datos privados, datos sensibles, *Habeas Data*, titulares, encargados y responsables de la información, intimidad, buen nombre.

[1] Universidad Católica de Oriente – Colombia. 24 de marzo de 2023.

[2] Estudiante de pregrado Universidad Católica de Oriente. andres.marin9439@uco.net.co
Docente asesor: Libardo Quintero Salazar.

ABSTRACT

If it is about valuable resources, for entities with a commercial spirit mainly, the personal information of their target audience is one of the most important. This is why most companies are now focused on having robust databases, which can be extremely valuable when used hand in hand with the technological development we currently have. However, the collection and use of this information has a legal regulation in Colombia to avoid violating the fundamental rights of citizens, such as privacy, free development of personality, good name, etc. An article is then presented in which the findings of an investigation are exposed, where the sanctioning procedures carried out by the Superintendence of Industry and Commerce (hereinafter SIC) between 2020 and 2022 were analyzed, seeking to identify which are the most recurring offenses. to the norm, which finally results in a sanction imposed by this surveillance and control entity.

KEY WORDS

Personal data, data processing, fundamental right, public data, semi-private data, private data, sensitive data, Habeas Data, owners, managers and managers of information, privacy, good name.

INTRODUCCIÓN

La Protección de los Datos Personales es uno de los derechos fundamentales que ha tenido desarrollo en Colombia a partir de la Constitución Política de 1991. Los datos personales son partes de información, con la cual puede ser identificada o identificable una persona, situación que cobra relevancia al momento de clasificar estos datos en públicos, semiprivados, privados y sensibles, pues como existen datos que cualquier persona puede conocer, existen otros que, de ser divulgados, pueden crear un perjuicio para el titular o dueño.

Es por esto, que en Colombia se han venido implementado normas para proteger la información personal, esto, a través de la SIC como la autoridad delegada para la protección de este derecho fundamental, que como se indica se encuentra en pleno desarrollo y conocimiento en el país, pues debo advertir que se percibe un ambiente de desconocimiento de la normatividad que existe, tanto por parte de los titulares de la información, como por parte de las entidades responsables o encargadas de su manejo y custodia.

Por su parte, la emergencia sanitaria que trajo el Covid-19, aumentó en gran medida la interacción a través de herramientas tecnológicas que al mismo tiempo posibilitan el intercambio de información acelerada, información personal que puede estar dentro de cualquiera de sus clasificaciones y que llega a ser utilizada para múltiples fines o actividades comerciales, en muchas ocasiones sin contar con la autorización expresa de su titular, generando un infracción a la Ley 1581 de 2012 y por consiguiente a las protecciones que desde la Constitución Política y posterior desarrollo jurisprudencial y normativo se le están otorgando a las personas.

Así las cosas, en el presente trabajo se pretende determinar cuáles son las conductas infractoras a la Protección de Datos Personales más recurrentes según las resoluciones sancionatorias publicadas por la SIC durante los años 2020 a 2022.

El presente escrito se desarrolla de la siguiente manera: se tocan primeramente los conceptos y generalidades sobre la Protección de Datos Personales, seguidamente se hace un recuento normativo y jurisprudencial de este derecho fundamental en Colombia, luego se hace un estudio de las decisiones administrativas emitidas por la SIC, para finalmente entregar unas conclusiones que permitan identificar las infracciones más recurrentes a este derecho en Colombia.

METODOLOGÍA

La información obtenida con esta investigación, se logró a través de un análisis documental realizado a las decisiones administrativas emitidas por la SIC entre los años 2020 y 2022. Es así, como el objetivo de este capítulo es explicar el proceso que se adelantó para identificar, estudiar y determinar cuáles fueron las conductas infractoras a la Protección de Datos Personales más recurrentes durante el mencionado periodo de tiempo.

En primer lugar, se identificaron los procedimientos sancionatorios adelantados por la SIC, los cuales son publicados por dicha entidad en su página web www.sic.gov.co. Allí se encuentran las decisiones administrativas emitidas por este ente de vigilancia y control desde el año 2014, así que se tomaron las que serían objeto de análisis y se continuó con la lectura de cada una. De esta lectura se hizo un resumen en donde se resaltaron los derechos vulnerados y las conductas que van en contra de las normas establecidas en Colombia para la protección de la información personal.

Una vez realizado el resumen e identificadas las conductas infractoras que llevaron a que la SIC adelantara la correspondiente investigación, se prosiguió a filtrar la información para destacar las conductas más recurrentes, de tal manera que, en el capítulo que se hará referencia a las infracciones, se describen las faltas más recurrentes a la normatividad.

CAPÍTULO I

GENERALIDADES DEL TRATAMIENTO DE DATOS PERSONALES

A continuación, se desarrollarán los principales conceptos sobre Datos Personales, ello con la intención de tener un marco general de aproximación al tema principal, que es el estudio de las principales infracciones a la Ley 1581 de 2012, la cual dicta disposiciones generales para la Protección de Datos Personales, todo esto desde los procedimientos sancionatorios tramitados en la SIC como la autoridad facultada por la ley para ejercer vigilancia y control sobre este tema.

En primer lugar, es necesario saber que un dato personal es una pieza de información que puede llegar a identificar en una pequeña o gran medida a una persona. Existen datos personales de diferentes clases y se categorizan según el nivel de riesgo al cual se puede exponer el titular al momento de entregar o no ese dato. De igual forma, los tipos de tratamiento de datos hacen referencia a las operaciones que se efectúan sobre los datos personales, se mencionan algunas de estas operaciones más adelante, pero no se agotan allí.

Las personas naturales o jurídicas propietarias de dichos datos personales tienen una serie de derechos sobre la manipulación de su información, derechos que están consagrados en la Ley 1581 de 2012, los cuales pueden verse afectados por el mal manejo de los datos personales y están estrechamente relacionados con las subcategorías del dato personal.

Existen diferentes modelos de protección a este derecho fundamental, en donde cada gobierno ha adoptado estrategias en cuanto al Tratamiento de los Datos Personales en la red, por lo cual se puede indicar que son desarrollos estratégicos, organizativos y aplicativos utilizados en las actuaciones referentes a Datos Personales y resalta los aspectos principales para una correcta gestión de los mismos.

1.1. TIPOS DE DATOS PERSONALES

Como he mencionado antes, los datos personales se clasifican en diferentes tipos, estos pueden ser públicos, semiprivados, privados y sensibles, y atienden al nivel de riesgo que se expone una persona al momento de darlos a conocer, por tanto, pasaré a definir cada uno de ellos ofreciendo algunos ejemplos.

En primer lugar, hablaremos de los datos públicos, los cuales son de libre circulación, estos facilitan el contacto con la sociedad y lo que prevalece es el derecho a la información. Normalmente están contenidos en registros o documentos públicos por lo tanto cualquier persona puede tener acceso a ellos sin que esto se considere un perjuicio para el titular. Algunos ejemplos de datos públicos pueden ser el número de identificación, nombres y apellidos, tipo de identificación, fecha y lugar de expedición, estado civil, nacionalidad, correo electrónico corporativo, teléfono o celular corporativo, dirección laboral, datos relativos a la actividad comercial o profesional, datos de afiliación a la EPS, etc. Piénsese en la información que se puede encontrar de las personas en registros públicos como los de la Cámara de Comercio cuando una persona tiene la calidad de comerciante o el registro inmobiliario, entre otros.

Por otro lado, encontramos los datos semiprivados, que se refieren propiamente a los que le interesan al titular de la información y a cierto grupo de personas o entidades en un momento específico, buscan proteger el buen nombre y para darse a conocer requieren autorización del titular. Los siguientes son algunos ejemplos: Edad, lugar y fecha de nacimiento, correo electrónico personal, teléfono o celular personal, estrato, ingresos y egresos, datos de afiliación EPS (Fecha de ingreso, retiro, novedades), comportamiento crediticio, historia laboral, experiencia laboral, llamados de atención, nivel académico, calificaciones, información tributaria, antecedentes judiciales y disciplinarios, entre otros.

También, encontramos que existen datos conocidos como privados, mismos que son de naturaleza íntima o reservada y sólo son relevantes para el titular, no se pueden solicitar de manera obligatoria, a no ser que sea por orden de autoridad judicial competente y en ejercicio de sus funciones y protege el derecho a la intimidad, como lo son los gustos, aficiones, contraseñas o patrones, llamadas telefónicas, textos de mensajería instantánea, contenido de correos electrónicos, historial de navegación, fotos (salvo cuando se tratan como datos sensibles para uso de autenticación biométrica), etc.

Por último, encontramos los datos sensibles que son aquellos que pueden afectar al titular, ya que si se divulgan pueden generar discriminación. Protegiendo estos datos se busca proteger la dignidad, la intimidad y la vida. Está prohibido el tratamiento de datos personales sensibles, a no ser que el titular otorgue una autorización expresa para este tratamiento. Algunos de estos son los datos biométricos (huella, ADN, imagen de vídeo, voz, siempre y cuando se pueda identificar ante un sistema de información), origen étnico, color de piel, señales particulares, estatura, peso, orientación sexual, orientación política o religiosa, entre otros.

1.2. TIPOS DE TRATAMIENTO DE DATOS

Sobre los datos personales se pueden efectuar diferentes operaciones, es decir pasan por un proceso que va de la mano con la clasificación de los mismos, esto para considerar que dentro de dicho "ciclo de vida de la información" casi siempre es necesario contar con la autorización del titular, así como atender sus solicitudes, además de cumplir con las obligaciones que la ley le impone a cada responsable de almacenar, conservar y tramitar la información.

La primera parte de este proceso se da en la recolección, etapa que atiende a la manera en cómo el responsable de la información recibe ciertos datos ya sea mediante encuestas, cookies, a través de terceros o ahora más usado a través de *Big Data* e IA (Inteligencia artificial). Vale recordar que esta es una de las etapas más importantes, pues la entidad o persona que recibe estos datos debe contar con la autorización previa e informada del titular de acuerdo a lo señalado en la ley, misma que además indica que esta autorización debe ser obtenida a través de un medio que pueda ser objeto de consulta posterior (Ley 1581 de 2012).

Después de la recepción de los datos personales, estos deben ser almacenados con la ayuda de mecanismos de seguridad técnicos y administrativos para que la información no sea filtrada o sea accedida por personal no autorizado, así como asegurarse que la circulación de esta información se dé entre personas o entidades autorizadas por el titular. Es muy importante señalar que el uso de los datos debe darse de acuerdo a la finalidad por la cual se recogió y por los cuales el titular autorizó, no se puede adquirir un dato para una finalidad específica y utilizarlo para algo diferente.

Finalmente, la información se puede archivar siempre y cuando exista una ley que obligue a conservarla, de lo contrario debe eliminarse una vez finalice su objetivo de gestión.

1.3. DERECHOS DE LOS TITULARES

La Ley 1581 de 2012 establece una serie de derechos que tienen los titulares de los datos personales y que deben ser respetados por los responsables de la información. Es decir que la relación del titular con su información no finaliza al momento de otorgar una autorización para que esta sea usada, almacenada o divulgada, sino que conserva la facultad de disponer sobre ella cuando la ley así lo permite.

Uno de los derechos que amparan al titular, es conocer la información que de él existe en ciertas bases de datos, para lo cual puede consultar la finalidad con la que se están usando los datos personales, qué tiempo los van a conservar y los canales dispuestos por el responsable para ejercer sus derechos.

De la misma manera, la ley otorga el derecho de actualizar y rectificar datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado. También se puede solicitar revocar y/o suprimir los datos cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales, siempre y cuando la SIC haya determinado previamente que el responsable del tratamiento ha incurrido en conductas contrarias a la ley. Existen otras facultades que la ley otorga a los titulares como lo es solicitar información, prueba de la autorización y ejercer el derecho de *hábeas data* ante la SIC cuando el encargado del tratamiento no da respuesta a la petición o el reclamo.

Todo titular puede ejercer estos derechos presentando una reclamación ante el responsable o encargado del tratamiento de los datos, el cual contará con un término de 15 días hábiles para atender y dar respuesta a la reclamación. De no emitirse una respuesta o la respuesta ser inadecuada, dicha reclamación se eleva ante la SIC.

Los derechos se vulneran cuando los datos recolectados no se usan para el fin definido violando la esfera de privacidad, cuando no se actualizan los datos solicitados, cuando no se toman las medidas necesarias para garantizar la protección de la información y cuando se entrega la información a terceros sin la previa autorización del titular, entre otras razones que generan sanción.

1.4. DEBERES DE LOS RESPONSABLES O ENCARGADOS DEL TRATAMIENTO

En el artículo 17 de la Ley 1581 se establecen los deberes del responsable del tratamiento de datos, las cuales versan sobre actuaciones que deben realizar los responsables o encargados del tratamiento de datos personales, para garantizar los fines establecidos en la Ley y atender adecuadamente las solicitudes de los titulares.

Entre los deberes mas relevantes que establece la Ley, está garantizar el derecho de *Habeas Data* que tiene el titular, esto es actualizar, corregir o suprimir la información que así se solicite, atendiendo de manera oportuna y eficaz, esta y otras solicitudes recibidas sin excederse de los términos señalados en la norma para tales fines.

Otros deberes son adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley, así como de las consultas y reclamos recibidos. De la misma manera, la ley exige a los responsables y encargados cumplir con unas condiciones de seguridad y privacidad de la información para evitar violaciones a estos datos, mismas que de llegarse a dar, deben ser informadas a las autoridades delegadas para la protección de datos.

1.5. DERECHOS IMPACTADOS

Seguidamente, trataremos algunos derechos que pueden verse afectados por el mal manejo de los datos personales, mismos que están estrechamente relacionados con las subcategorías del dato personal.

Uno de los derechos más importantes al momento de referirnos a información personal, es el derecho a la intimidad, siendo incluso uno de los primeros que se discutió y dio lugar a la creación de normas para proteger el habeas data. Se encuentra consagrado en la Declaración Universal de Derechos del Hombre en 1948, la cual estipula en su artículo 12 lo siguiente:

> 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 o ataques.

Es importante resaltar lo dicho por la Corte Constitucional al referirse al derecho a la intimidad:

> El derecho a la intimidad, está orientado a garantizar a las personas una esfera de privacidad en su vida personal y familiar, al margen de las intervenciones arbitrarias del Estado o de terceros. Comprende de manera particular la protección frente a la divulgación no autorizada de los asuntos que conciernen a ese ámbito de privacidad. (CConst., C-489/22, R. Escobar).

Esto debe adaptarse a las dinámicas sociales, por lo tanto, esta protección debe llevarse al espacio cibernético y aún más con el acelerado desarrollo tecnológico que se está dando en la actualidad. Así entonces, podemos encontrar un amplio desarrollo jurisprudencial de este derecho que busca principalmente proteger a las personas de cualquier tema que atente contra su honra y reputación.

El libre desarrollo de la personalidad es otro derecho que se busca proteger con la información personal, este se encuentra consagrado en el artículo 16 de la Constitución Política de 1991 y se trató también por parte de la Corte Constitucional en 1998, así:

> El derecho fundamental al libre desarrollo de la personalidad protege la capacidad de las personas para definir, en forma autónoma, las opciones vitales que habrán de guiar el curso de su existencia. En esta medida, ha señalado que, en el artículo 16 de la Carta Política, se consagra la libertad in nuce, toda vez que cualquier tipo de libertad se reduce finalmente a ella o, dicho de otro modo, la anotada norma constitucional constituye una cláusula general de libertad. Así caracterizado, el derecho al libre desarrollo de la personalidad presupone, en cuanto a su efectividad, que el titular del mismo tenga la capacidad volitiva y autonomía suficientes para llevar a cabo juicios de valor que le permitan establecer las opciones vitales conforme a las cuales dirigirá su senda existencial. (CConst., SU 642/98, E, Cifuentes).

Este derecho también es conocido como derecho a la autonomía e identidad personal y tiene un amplio desarrollo jurisprudencial en el que se destaca el respeto por los intereses y convicciones de las personas siempre y cuando este cuente con las capacidades suficientes para tomar sus propias decisiones y dichas actuaciones respeten los derechos ajenos.

Así mismo, encontramos el derecho al buen nombre, definido en la Sentencia C-489 del 2002 como:

> La reputación, o el concepto que de una persona tienen los demás y que se configura como derecho frente al detrimento que pueda sufrir como producto de expresiones ofensivas o injuriosas o informaciones falsas o tendenciosas. Este derecho de la personalidad es uno de los más valiosos elementos del patrimonio moral y social y un factor intrínseco de la dignidad humana que a cada

> persona debe ser reconocida tanto por el Estado, como por la sociedad. El derecho al buen nombre, como expresión de la reputación o la fama que tiene una persona, se lesiona por las informaciones falsas o erróneas que se difundan sin fundamento y que distorsionan el concepto público que se tiene del individuo. (Corte Constitucional, 2002).

De tal manera que este derecho se enfoca en proteger a las personas frente a expresiones o informaciones ofensivas o injuriosas, falsas o tendenciosas, o que se tiene derecho a mantener en reserva, las cuales distorsionan el concepto público que se tiene del individuo o titular.

El derecho al *Habeas Data* podría considerarse como la adaptación del *Habeas Corpus* al espacio digital, este es un derecho fundamental que tiene toda persona para conocer, actualizar y rectificar toda aquella información que se relacione con ella y que se recopile o almacene en centrales de información. Este derecho está regulado por el Artículo 15 de la Constitución Política de Colombia, desarrollado por la Ley 1266 de 2008. Según la Corte Constitucional, el núcleo esencial del habeas data se encuentra integrado por el derecho a la autodeterminación informática, entendiendo esto como la facultad de la persona, para autorizar la conservación, uso y circulación de sus datos y a la libertad, en especial la económica, ya que esta podría ser vulnerada en virtud de la circulación de datos que carezcan de veracidad o para los cuales no se haya autorizado su circulación.

> La Corte señaló que el habeas data, como derecho autónomo o instrumento para proteger otras prerrogativas, es una garantía que salvaguarda la libertad de la persona, entendida no como posibilidad de locomoción sin restricciones, sino como la extensión que se hace de ella en medios virtuales o físicos de acopio de datos personales, en los cuales se construida o proyectada a través de la diferente información que se ha recogido de sí. De ahí que también reciba el nombre del derecho a la "autodeterminación informática". (CConst., T-509/20, J. Reyes).

Otro derecho importante es el derecho a la información, en donde vale anotar que la información que fluye por el ciberespacio, constituye un bien material y moral que es patrimonio de la humanidad, como también lo es el ciberespacio. El acceso a dicha información y al propio ciberespacio, es un derecho universal que debe ser facilitado a todas las personas, no obstante, ello tiene algunas restricciones que como ha indicado la Corte, "persiguen una finalidad constitucional, pues con ella se pretende proteger el derecho a la intimidad de las víctimas, de conformidad con el artículo 15 Superior" (Sentencia T-828/14, G. Ortiz).

Podremos concluir entonces, que el derecho a la información se constituye como un derecho importante que impulsa el ejercicio de la participación ciudadana, pero que, como ha indicado la Corte Constitucional, tiene restricciones principalmente al momento de involucrar la esfera privada de las personas, otra afirmación deja ver la relevancia que tiene la adecuada protección de la información personal de acuerdo a las diferentes clasificaciones de los datos.

1.6. MODELOS DE PROTECCIÓN DE DATOS PERSONALES

Cada gobierno ha adoptado estrategias en cuanto al tratamiento de los datos personales en la red, por lo cual se pueden definir como desarrollos estratégicos, organizativos y aplicativos dirigidos a las actuaciones en cuanto a datos personales y resalta los aspectos principales para una correcta gestión de los mismos.

En Europa, es utilizado el modelo centralizado que busca reconocer los datos personales para su defensa y darle categorías, estructurando sistemas gubernamentales que cuentan con una autoridad central, una categoría común de datos personales, unos principios generales de obligatorio cumplimiento y las respectivas garantías para los interesados o titulares de la información.

Por su parte, Estados Unidos adoptó un modelo sectorial, que busca proteger esta información como su nombre lo indica, con autoridades ubicadas por sectores estratégicos cada una con su regulación. No hay categorías comunes de datos personales y se cuentan con algunas garantías para los interesados.

Y, finalmente, Colombia cuenta con un modelo híbrido. Esto implica que existe una ley sectorial relativa al Habeas Data Financiero (Ley 1266 de 2008) y una ley general en protección de datos personales (Ley 1581 de 2012). Existen entonces autoridades sectoriales y una autoridad central y una categoría común de datos personales. Esta regulación sectorial y regulación general busca una constante garantía para los interesados o titulares de la información.

1.7. REGISTRO NACIONAL DE BASES DE DATOS

Los datos personales han adquirido una importancia creciente en la actualidad, dado que el tratamiento de la información de las personas debe tener una regulación legal, por ello se creo el

Registro Nacional de Bases de datos, un directorio público de las bases de datos que operan en Colombia, el cual es administrado por la SIC.

Este registro sirve para conocer la realidad de las bases de datos del país, la cantidad de titulares y tipos de datos tratados, así como quien o quienes adelantan su tratamiento, la finalidad y las políticas de tratamiento y los canales y mecanismos dispuestos para recibir consultas, peticiones y reclamos entre otros aspectos. Su utilidad principal es crear conciencia sobre el manejo adecuado de la información personal contenida en bases de datos.

El régimen general de Protección de Datos Personales, es aplicable a todas las sociedades y entidades de Colombia sin excepción, por su parte, el proceso de registro en el Registro Nacional de Bases de Datos, lo deben llevar a cabo únicamente las sociedades y entidades sin ánimo de lucro que tengan más de 100.000 Unidades de Valor Tributario (UVT) de activos totales como lo establece el Decreto 090 de 2018 independientemente del número de empleados que tengan a la fecha y las entidades públicas.

Las bases de datos objeto de inscripción, son aquellas que contengan datos personales cuyo tratamiento autorizado o manual se realice por personas naturales o jurídicas de naturaleza pública o privada en el territorio colombiano o fuera de él. En este último caso siempre que le responsable o el encargado del tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internaciones.

1.8. LA SIC Y LA PROTECCIÓN DE DATOS PERSONALES

La Superintendencia de Industria y Comercio (SIC) es el ente administrativo delegado para el control y supervisión del Tratamiento de Datos Personales en Colombia, así lo estableció la Ley 1266 de 2008 y la Ley 1581 de 2012, en sus artículos 17 y 19 respectivamente:

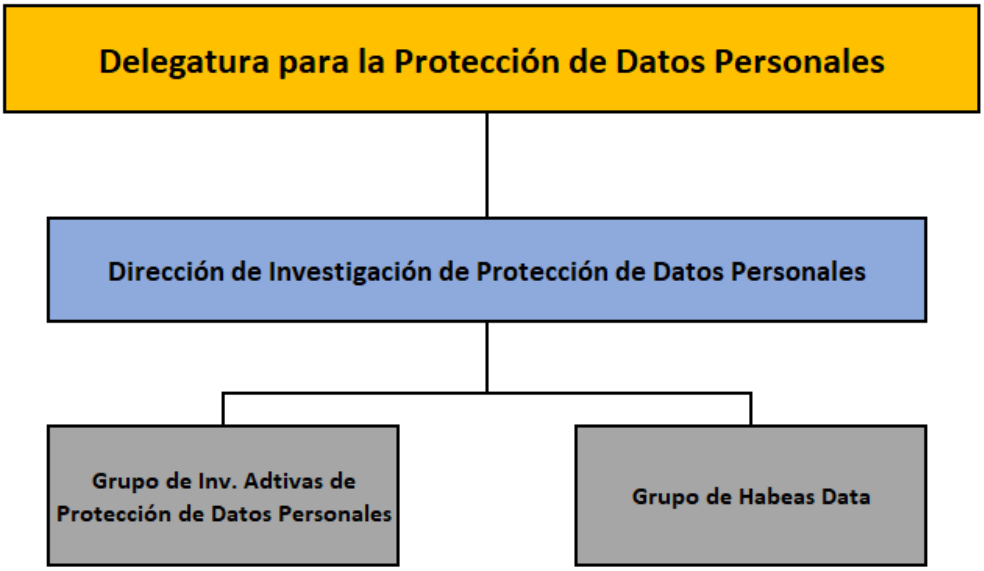
> Artículo 17 Ley 1266 de 2008. *Función de vigilancia*. La Superintendencia de Industria y Comercio ejercerá la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales que se regula en la presente ley.

> Artículo 19 Ley 1581 de 2012. *Autoridad de Protección de Datos*. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

Este es un ente de vigilancia y control que tiene facultades sancionatorias que puede materializar en busca de proteger los derechos de los colombianos relacionados con su información personal, a través de su delegatura para la Protección de datos Personales, misma que fue creada en el año 2011 por medio del Decreto 4886 de 2006. Las funciones que tiene la Delegatura en mención, son principalmente la vigilancia de los operadores, fuentes y usuarios de información relacionada con el cumplimiento e incumplimiento de obligaciones dinerarias, así como la supervisión del cumplimiento de las instrucciones que emita la SIC. Igualmente, este ente administra el Registro Nacional Público de Bases de Datos, lleva a cabo las investigaciones y sanciona si ello es procedente después de realizar auditorías para verificar el cumplimiento de las normas sobre protección de datos personales.

Este organismo público adscrito al Ministerio de Comercio, Industria y Turismo, en relación con el tratamiento de datos personales, también busca garantizar que, en la recolección, el uso, la circulación y el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la Constitución y en la Ley (Derecho al debido tratamiento de datos personales). Otra de sus funciones es exigir el respeto del habeas data previsto en el artículo 15 de la Constitución Política Nacional, el cual permite a la persona 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.

El equipo de trabajo que tiene dedicado la SIC para la protección de los datos personales, se dedica principalmente a velar por el cumplimiento de la legislación en materia de protección de datos personales, adelantar investigaciones sobre presuntas vulneraciones de la regulación de tratamiento de datos personales y ordenar las medidas que sean necesarias para hacer efectivos los derechos fundamentales al *Hábeas Data* y al debido tratamiento de datos personales. En la siguiente gráfica, se puede observar la estructura al interior de la SIC delegada para la Protección de los Datos Personales de los colombianos:



CAPÍTULO II
ANTECEDENTES NORMATIVOS Y JURISPRUDENCIALES DEL TRATAMIENTO DE DATOS PERSONALES EN COLOMBIA

2.1. ANTECEDENTES NORMATIVOS Y JURISPRUDENCIALES DE LA PROTECCIÓN DE DATOS PERSONALES

Al tratar este tema, es normal que muchas personas piensen que se trata de una regulación nueva y que solo hasta ahora se le ocurre al derecho buscar proteger la intimidad de las personas, pero la protección de datos personales tiene antecedentes que se remiten muchos años atrás, iniciando con la Declaración Universal de los Derechos Humanos en 1948, el cual por primera vez, mencionó el derecho a la intimidad en su artículo 12, aspecto que fue ratificado en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de las Naciones Unidas en 1966, mismo que sería posteriormente el artículo 11 de la Convención Americana de Derechos Humanos de 1969.

En la Unión Europea, la protección de este derecho empezó a desarrollarse en 1950, al reconocerse en derecho a la intimidad en el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, de la misma manera que el Consejo de Europa en 1968 busco la protección de este derecho mediante la Resolución 509 de cara a los avances tecnológicos

acelerados que amenazaban los derechos fundamentales de las personas. A partir de allí, la Unión Europea emite una legislación muy importante que llevó a desarrollar el concepto de protección de datos personales como se conoce hasta ahora, todo esto, como ya lo mencioné, debido principalmente al acelerado intercambio de información a la mano de la evolución de tecnologías en Europa. (Bermúdez Durana, 2011).

Por su parte, en América Latina se dio lugar a la XIII Cumbre Iberoamericana de Jefes de Estado de Gobierno en 2003, siendo este el primer escenario en el que se planteó la necesidad de proteger los datos personales como un derecho fundamental. Esto dio lugar a que cada país de este territorio iniciara un desarrollo más amplio de estos derechos que muchos ya habían mencionado en su constitución Política, como facultades para conocer los datos contenidos bases de datos públicas y privadas, conocer la finalidad del uso de datos, exigir actualizaciones, exigir confidencialidad, etc.

En Colombia particularmente, el Tratamiento de Datos Personales está fundamentado desde los artículos 15 y 20 de la Constitución Política, los cuales rezan lo siguiente:

> Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
>
> La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o 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.
>
> Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

Posteriormente se ha desarrollado este tema a partir de la Sentencia T-414 de 1992, considerada como una garantía del derecho a la intimidad que debe ser respetado por el mismo Estado y los particulares. A partir de 1995 el derecho al Habeas Data empezó a comprender las facultades del titular para conocer su información recopilada, actualizarla y rectificarla, además de considerarse en adelante un derecho autónomo, todo esto gracias a la Sentencia SU-082.

En el año 2002, la Corte a través de la Sentencia T-729 indico algunas diferencias fundamentales entre el derecho de Hábeas Data y otros derechos como la intimidad o el buen nombre, encontrando allí que los aspectos más relevantes son la posibilidad que tiene el titular de la información para proteger su derecho de Hábeas Data incluso a través de acción de tutela y las particularidades del régimen jurídico aplicable a la hora de buscar su protección constitucional.

La autonomía de este derecho fundamental fue ratificada por la Corte Constitucional en el año 2008 a través de la Sentencia C-1011, la cual otorgó facultades para conocer, incluir, actualizar, rectificar, corregir y excluir información por parte del titular ya sea porque se esté haciendo un mal uso de ella o simplemente por voluntad del dueño de la información.

Posteriormente llegaría la Ley Estatutaria 1266 de 2008 y sus Decretos reglamentarios 1727 de 2009 y 2952 de 2010. Vale anotar que antes de la expedición de esta Ley habían sido radicados doce proyectos en la Cámara de Representantes y en el Senado de la República, los cuales no lograron hacer tránsito legislativo y se quedaron en diferentes momentos y etapas procesales, pero que mostraron la preocupación del órgano legislativo colombiano por regular este tema. Fue así como se dio inicio a la protección de datos personales en Colombia mediante una Ley Estatutaria, no obstante, esta Ley se quedó corta, pues estaba orientada exclusivamente a la protección de datos comerciales y financieros.

Pasarían cuatro años más para que se expida la ley 1581 de 2012, en la cual se regula el derecho fundamental de Habeas Data con la finalidad de proteger los datos personales registrados en cualquier base de datos que permita realizar operaciones como recolección, almacenamiento, uso y tratamiento por parte de entidades de naturaleza pública y privada. Esta Ley que sigue vigente al día de hoy y es considerada el centro normativo de la protección del derecho de Hábeas Data en Colombia, fue reglamentada a través del Decreto 1377 de 2013, que además obliga a las empresas

que cuenten con datos almacenados desde antes de la expedición de esta norma, a conseguir la autorización de los titulares.

CAPÍTULO III

INFRACCIONES A LA LEY DE PROTECCIÓN DE DATOS PERSONALES (LEY 1581 DE 2012) EN LOS PROCEDIMIENTOS SANCIONATORIOS TRAMITADOS POR LA SIC ENTRE LOS AÑOS 2020 Y 2022.

Como he mencionado en este escrito, la SIC a través de su delegatura para la Protección de Datos Personales, es el ente administrativo delegado para el control y supervisión de este derecho fundamental en Colombia, tal como lo establece la normatividad vigente de este país. De tal manera, que el presente capítulo está destinado a presentar las sanciones impuestas por esta entidad durante los años 2020 a 2022, exponiendo algunas de las sanciones más relevantes de cada anualidad.

3.1. ALGUNOS CASOS DE RELEVANCIA AÑO 2020.

En el año 2020 la SIC emitió 48 decisiones administrativas en donde se impusieron sanciones por la vulneración del derecho fundamental del habeas data, dentro de las principales causales están la no atención a solicitudes del titular de la información para que esta sea corregida, actualizada o suprimida, así como el envió de publicidades y mensajes comerciales sin contar con la autorización y la no respuesta a requerimientos en el término estipulado por la ley. A continuación, presentaré algunos de los casos más interesantes de esta anualidad.

- *Caso Scotiabank Colpatria S.A.*

El grupo de trabajo de la SIC inició investigación administrativa a la entidad BANCO COLPATRIA después de recibir una denuncia donde un ciudadano manifestó recibir promociones comerciales en su celular constantemente, sin que se limiten de continuar haciéndolo después de solicitar esto a la entidad en varias oportunidades. Adicionalmente manifestó que solicitó copia de

la autorización para el tratamiento de sus datos personales y nunca le fue allegada. Finalmente manifestó que el banco le informó que ya habían sido suprimidos sus datos y a pesar de ello continuó recibiendo mensajes comerciales.

Después de tener la posibilidad de presentar sus descargos, la SIC consideró que la entidad no pudo demostrar que sus actuaciones estuvieran ajustadas a derecho, pues no se logró probar que contaba con la autorización del titular para almacenar y usar su información personal. Fue entonces cuando se le impuso una sanción de 356 millones de pesos.

Este caso expone algunas de las infracciones más comunes en materia de protección de datos personales, ya que frecuentemente las entidades no adoptan procedimientos adecuados para recibir la información de los titulares y tramitar la autorización de este que faculte a la entidad para conservar esa información y usarla para ciertos fines. De la misma manera, nos presenta las dificultades que comúnmente tienen estos titulares de la información cuando quieren hacer uso de los derechos que les otorga la Ley 1581 de 2012, en este caso, la de solicitar la supresión de sus datos.

- *Caso Colombia Móvil S.A. ESP*

En este caso, una mujer solicitó a la entidad COLOMBIA MÓVIL conocida como TIGO, que eliminara la dirección de su domicilio de su base de datos, ya que estaban llegando constantes facturas a su vivienda a nombre de una persona que desconoce. Indicó que la entidad respondió positivamente a su solicitud, pero a pesar de ello, siguieron llegando los mismos documentos a su domicilio.

Por su parte, COLOMBIA MÓVIL indicó en su oportunidad de descargos que la persona denunciante no ha tenido relaciones contractuales con la entidad, por tanto, no se podría inferir tratamiento alguno a sus datos personales.

Posteriormente la SIC corrió traslado de las pruebas a la sociedad investigada en donde le solicitó pronunciarse al respecto de los datos incorporados en las facturas que indica recibir la titular de la información, para lo cual la entidad guardó silencio. Dando lugar a la SIC para concluir con el respectivo análisis del caso, que efectivamente se vulnero el derecho de hábeas data del titular pues

este no tiene que insistir para que sus derechos sean garantizados. Por el contrario, estos deben ser salvaguardados sin dilación alguna por parte de los responsables o encargados del tratamiento, siendo sancionada pecuniariamente con 50 millones de pesos.

Claro caso para dimensionar la importancia de acatar adecuadamente las solicitudes de los titules y dentro de los términos establecidos en la ley, pues la omisión de estas solicitudes da pie a que el titular presente queja ante la SIC y se inicie una investigación en la que muchas veces las empresas no logran sustentar de manera suficiente y válida, y no dan cuenta del uso que se le está dando a la información que tiene en su base de datos ni la autorización del titular para hacerlo.

- *Caso Banco de Bogotá S.A.*

Una ciudadana denuncia ante la SIC, que la entidad BANCO DE BOGOTÁ viene realizando llamadas y enviando mensajes de texto a su celular realizando cobros amenazantes e intimidatorios, a los cuales ha indicado verbalmente al banco que no cuenta con ningún tipo de servicio ni relación contractual con ellos, solicitando que se abstengan de usar su línea móvil sin su autorización.

En la oportunidad procesal pertinente, la entidad indicó que el número móvil de la denunciante fue suministrado por su hijo, quien actualmente presentaba mora en el pago de sus obligaciones con el banco y quien suministró dicho medio para establecer comunicación con él, no obstante, no aportaron una autorización válida por parte de la titular de la línea móvil para alegar que no se estaba infringiendo su derecho de hábeas data. Por tanto, la SIC concluyó que la denunciante no tenía relación directa con el banco y este no contaba con su autorización para contactarla a ella o terceros a través de este medio, así, impuso una sanción por un valor de 351 millones de pesos.

Este caso presenta la necesidad que tienen las entidades receptoras de datos personales para tomar adecuadamente la autorización del titular y poder hacer uso de su información, corroborando que ésta efectivamente corresponde a la persona que mantiene una relación comercial con la entidad. Adicionalmente se evidencia una vez más, la importancia de respetar el derecho de hábeas data, esto es, acatar las solicitudes de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada.

Como ya lo indiqué, fueron 48 las sanciones impuestas por la SIC durante esta anualidad, de las cuales tomé algunas que tienen un desarrollo interesante según los objetivos propuestos en la investigación. De tal manera, que durante el año 2020 predominó la falta de autorización del titular de la información para que las entidades hagan uso de ella, así como la falta de atención oportuna a los requerimientos que estos hacen para que su información sea corregida, actualizada o suprimida.

3.2. ALGUNOS CASOS DE RELEVANCIA AÑO 2021.

A continuación, haré el mismo análisis que vengo realizando con las sanciones impuestas durante el año 2021. Valga anotar que para este periodo de tiempo se impusieron 64 sanciones, representando un aumento del 30.7% en relación con el año anterior. Así mismo, haré un breve análisis de algunas sanciones impuestas durante este periodo de tiempo, en donde se siguieron presentando las mismas falencias del año 2020 y aumentaron las infracciones en otras etapas, como lo es en la política de privacidad que deben implementar las entidades, el no cumplimiento con el Registro Nacional en Bases de Datos y la no respuesta a los requerimientos de la SIC.

- *Caso Bimbo de Colombia S.A.*

Dos empleados de la entidad BIMBO DE COLOMBIA, elevan petición a la compañía solicitando se indique la finalidad y el uso que le dan a su información personal recolectada con la frecuente instalación de cámaras de video y vigilancia, quien es el responsable del tratamiento de los datos allí recolectados y porque es notorio que los jefes de planta y otras personas tienen acceso a dicho material.

La entidad presentó escrito en donde indicó que efectivamente cuenta con la autorización para tratar los datos personales de los colaboradores, no obstante, no dio respuesta a la solicitud hecha por ellos dentro del término legal, considerando que la petición no estaba direccionada a corregir, modificar o suprimir la información, indicando que no buscaba la protección del derecho fundamental de habeas data sino que debía tramitarse como derecho de petición en términos del artículo 23 de la Constitución Política.

Posición que no está ajustada a derecho según lo expuesto por la SIC pues la no respuesta a la petición vulnera el derecho que tienen todos los titulares de la información para conocer y ser informados respecto del uso que se les da a sus datos personales. De otro lado, la SIC determinó que los avisos de privacidad no cumplían en su totalidad con los requisitos mínimos impuestos en el decreto 1074 de 2015, por ejemplo, la falta de claridad en los mecanismos dispuestos por el responsable para que el titular conozca la política de tratamiento de la información, ni tampoco se deja claridad en el nombre del responsable del tratamiento. Por lo anterior, esta entidad administrativa impuso una sanción por 108 millones de pesos.

Este es un caso muy interesante para tratar y comprender el tema de las cámaras de video y los datos biométricos. En esta ocasión se hacía referencia a unas cámaras instaladas al interior de una compañía que a pesar de tener implementados los avisos de privacidad, estos no cumplían con todos los requisitos que pide la norma, avisos que también se deben implementar en instalaciones a las que accedan personas que no tengan vínculo con la entidad.

- *Caso Rappi S.A.S.*

En esta oportunidad el denunciante manifiesta que la entidad RAPPI continúa enviando mensajes de texto a pesar de contestar sus mensajes con la inconformidad de seguir recibiéndolos. Adicionalmente indica que en su página web no aparece el correo de servicio al cliente para elevar la solicitud.

La SIC abrió la respectiva investigación y determinó que la sociedad no ejecutó dentro del plazo máximo legal establecido la supresión de datos personales del titular. Por tal razón, incumplió el literal a) del artículo 17, en concordancia con el literal e) del artículo 8 de la Ley 1581 de 2012 y con el artículo 2.2.2.25.2.6 del Decreto Único Reglamentario 1074 de 2015, lo que le trajo como consecuencia una sanción de 280 millones de pesos.

Nuevamente se trae a colación un caso en el que no se atiende de manera oportuna el requerimiento del titular de la información, vulnerando su derecho de hábeas data y teniendo como consecuencia una sanción económica bastante considerable. Estos casos muestran la importancia que tiene la creación de áreas encargadas del manejo de la información personal dentro de las compañías, pues las sanciones a las que se exponen son bastante altas.

- *Caso Clínica Reyes S.A.S.*

Esta vez, la SIC en ejercicio de sus funciones de vigilancia y control, procedió a examinar la información cargada en el Registro Nacional de Bases de Datos por parte de la sociedad CLÍNICA REYES, evidenciando preliminarmente que esta sociedad no cumplió con el deber de realizar la inscripción en dicho registro. Así que, para efectos de verificar el cumplimiento de los deberes a cargo de la sociedad en mención, requirió a la clínica para que informara las razones de su incumplimiento y copia de las políticas y manuales que adoptan para el manejo de los datos personales que almacenan.

Este ente administrativo solicitó a la sociedad en repetidas ocasiones, pero esta siempre guardó silencio. Fue entonces como se inició una investigación y se demostró que la sociedad investigada no atendió el requerimiento del Despacho y, que, al estar obligada a registrarse en el Registro Nacional de Bases de Datos, no había documentado los procedimientos solicitados, siendo sancionada con casi 5 millones de pesos.

La falta de implementación de políticas y manuales para tramitar y gestionar la información personal de la que se sea responsable, hace frecuente que las entidades eviten dar respuesta a los requerimientos de la SIC. Es importante destacar en este caso que no siempre se inicia una investigación a partir de una queja, sino que la SIC cuenta con las facultades para hacer requerimientos de oficio y su desacato, seguramente acarreará sanciones.

- *Caso Grupo Éxito S.A.*

En este caso, nuevamente se hace referencia a solicitudes que no se atienden en debida forma por parte de los encargados o responsables de los datos personales. Esta vez, la denunciante indica que durante más de un año le solicitó a el GRUPO ÉXITO que eliminara su número de teléfono personal de sus bases de datos y evitara continuar enviando mensajes de texto con información publicitaria. Indicó que había recibido cuatro respuestas de dicha sociedad, todas informando que procederían con la eliminación de sus datos personales, pero indica que los mensajes continuaron llegando.

La investigación se llevó a cabo conforme al procedimiento establecido y concluyó en una sanción por 152 millones de pesos a esta sociedad al probarse que no acató la solicitud conforme lo establece la norma.

Hasta acá, se empiezan a identificar infracciones que son recurrentes y que se van convirtiendo en el factor denominador, o de otra manera, en las más comunes, lo que nos va llevando a obtener conclusiones y dar respuesta a la pregunta inicial que dio pie a este texto de reflexión.

3.3. ALGUNOS CASOS DE RELEVANCIA AÑO 2022.

Para referirme a los procedimientos del año 2022, es importante anotar que según los reportes publicados en la página web de la SIC, al momento de realizar esta investigación se encontró que todos los procesos para el año en estudio se encuentran "EN TRÁMITE", por tanto, no se contó con decisiones en firme para compararlas con los años anteriores. No obstante, rescato los 71 casos que a la fecha se encuentran en estudio, pues ello mantiene evidente el aumento en las infracciones año tras año.

3.4. PROCEDIMIENTOS EN TRÁMITE.

En este apartado de la investigación, quiero referirme a los procedimientos que la SIC tiene "EN TRÁMITE" al momento de esta consulta, pues los números antes mencionados por cada año, hacen referencia a las sanciones que se encuentran EN FIRME y si bien no dejan de ser números alarmantes, ello aumenta al sumarles los procesos que se encuentran en estudio y que probablemente terminen emitiendo una sanción como los demás.

Si bien en el año 2020 las SIC reporta que todos los casos se encuentran finalizados (en firme), para el año 2021 registra 7 casos aun investigación y para el 2022, como ya lo mencioné, los 71 casos registrados aun no finalizan. Reitero que estos casos son adicionales a los que se encuentran culminados y analizados en los numerales anteriores de este capítulo, dejando ver un aumento considerable en los casos repostados con este ente administrativo cada año, lo que deja ver la relevancia que este tema viene tomando a partir de su reglamentación.

Vale anotar que la SIC presenta un reporte en su página web de las decisiones administrativas en este tema desde el año 2014, registrando aumentos en los mismos, año tras año, en los cuales se evidencia un crecimiento en escala desde entonces, con una cantidad de 10, 7, 14, 16, 37, 61, 48, 64 y 71 procesos sucesivamente hasta ahora.

CONCLUSIONES

El Tratamiento de Datos Personales no es un tema reciente, pues a pesar de que Colombia no hace muchos años cuenta con leyes que lo regulan, este tiene un desarrollo jurisprudencial muchos más antiguo, especialmente a partir de la promulgación de la Constitución Política de 1991 la cual enfatizo en el derecho a la intimidad personal y familiar y el derecho al buen nombre, siendo este el fundamento o el inicio del desarrollo posterior que se daría a este tema en nuestro país y que hasta hoy, sigue cobrando importancia, también gracias al acelerado desarrollo tecnológico que trae tantas facilidades para intercambiar información.

En Colombia las facultades de supervisión y control sobre la Protección Datos Personales las tiene las Superintendencia de Industria y Comercio según lo ha establecido la Ley 1266 de 2008 y 1581 de 2012, en sus artículos 17 y 19 respectivamente. Este ente administrativo entonces, tiene facultades sancionatorias que puede materializar en busca de proteger los derechos de los colombianos relacionados con su información personal, a través de su delegatura para la Protección de datos Personales, misma que fue creada en el año 2011 por medio del Decreto 4886 de 2006.

Desde el año 2014, la SIC viene publicando las decisiones administrativas que adelanta a través de su página web, evidenciando un crecimiento constante año tras año, pues inicialmente se adelantaban entre 7 y 16 investigaciones por año y, desde 2019 se adelantan entre 48 y 71 procesos por cada anualidad. Estas cifras dejan ver la relevancia que el Tratamiento de Datos Personales viene tomando en Colombia, pues a partir de la reglamentación que ha tenido el tema se viene dando un incremento notorio en las infracciones.

Durante el año 2020, la SIC impuso 48 sanciones, entre las cuales se evidencia que las infracciones más recurrentes son la falta de autorización del titular de la información para que las entidades

hagan uso de ella, así como la falta de atención oportuna a los requerimientos que estos hacen para que su información sea corregida, actualizada o suprimida.

En el año 2021, se impusieron 64 sanciones, representando un aumento del 30.7% en relación con el año 2020. Se siguieron cometiendo las mismas infracciones en gran proporción sumado a otras, como lo es en la no implementación de la Política de Privacidad, el no cumplimiento con el Registro Nacional en Bases de Datos y la no respuesta a requerimiento de la SIC.

Para el año 2022, se encontró que todas las sanciones se encuentran en trámite, no obstante, hay 71 procesos que a la fecha están en estudio. Si bien no se pudo establecer las infracciones más recurrentes para este año, el número de procesos pendientes por concluir muestra un aumento evidente de los tramites que está realizando la SIC cada año y seguramente de las infracciones a la normatividad de Protección de Datos.

De tal manera, que las quejas más recurrentes ante la SIC son el desacato de los responsables de custodia de la información para atender requerimientos corrección, actualización o supresión de los datos, esto como consecuencia en la mayoría de las veces, debido las constantes llamadas o mensajes con fines comerciales que acostumbran realizar las entidades, ocasionando que las personas busquen evitar tales acercamientos. De tal manera que al ser conocido cada caso por la SIC esta inicia una investigación en donde cada responsable tiene la posibilidad de presentar sus descargos y material probatorio para justificar el uso que se está dando a tal información, evidenciando en el presente estudio que la toma de la autorización es quizás la principal infracción que se está cometiendo a la ley, pues al momento de ser requerida por este ente administrativo, difícilmente se logra acreditar la tenencia y la adecuada toma de la autorización, conforme a lo establecido por el artículo 9 de la Ley 1581 al señalar que esta debe ser previa al tratamiento de sus datos e informada al titular y que, puede ser obtenida a través de cualquier medio siempre y cuando pueda ser objeto de consulta posterior.

Otras infracciones que llaman la atención por su recurrencia, son la no inscripción de la información en el Registro Nacional de Bases de Datos por parte de los responsables, dentro del tiempo y condiciones establecidas por la norma, y, el desacato o no pronunciamiento a los requerimientos que hace la SIC a través de las facultades que tiene para hacerlo de oficio.

Así pues, esta investigación permite evidenciar los esfuerzos que el legislador ha realizado para regular el Tratamiento de Datos Personales en Colombia, avances que siguen siendo lejanos a los implementados por otros países especialmente europeos, pero que en mi concepto han forjado una línea base para que la información se empiece a tratar en debida forma, además en cabeza de la SIC como un ente administrativo serio y riguroso en las competencias que le ha otorgado la Ley.

Otro aspecto a destacar, es sin duda el creciente conocimiento que han ido adquiriendo los ciudadanos en relación con sus datos personales, pues si bien la SIC tiene facultades para iniciar procesos investigativos como ya lo mencioné, la mayoría de decisiones sancionatorias estudiadas se dieron en razón a una solicitud o queja interpuesta con anterioridad, que dio pie a un estudio de la Superentendía y un posterior requerimiento a la entidad.

De otro lado, preocupa la cantidad de infracciones que se cometen a la Ley por parte de las entidades receptoras de información y por tanto responsables de su debido uso. Infracciones que inician desde la inadecuada toma de la autorización por parte del titular, seguido de políticas de privacidad mal implementadas que no permiten evidenciar las finalidades y derechos que tiene cada titular de la información, lo que posteriormente genera una reclamación, pues es común que estos datos se utilicen para fines comerciales sin contar con el consentimiento de la persona, sumado al desacato que es frecuente cuando el titular quiere ejercer su derecho de habeas data, esto es, de corregir, actualizar o suprimir sus datos. De tal manera que de las infracciones estudiadas se puede deducir poco interés por parte de los responsables para implementar las políticas y requerimientos normativos en este tema, y/o un desconocimiento amplio en el sector comercial que ha ido implementando políticas a medidas que las personas conocen los derechos que les da la ley.

Finalmente, es infaltable mencionar que la pandemia ocasionada por el Covid-19 sin duda generó una necesidad un más acelerada para interactuar a través de medios no procesionales, por tanto, la tecnología hizo presencia de manera aún más habitual entre nosotros y así la necesidad de usarlas y aprender de ella, incluso por personas que nunca se vieron interesadas en ese mundo digital. Este factor, cobra relevancia en las infracciones que publica la SIC y que realizara en adelante, pues sin duda las infracciones han sido considerables y de frente a una pandemia muchos desarrollos e interacciones han sido acelerados, lo que habilita aún más las posibilidades de infringir la normatividad vigente.

BIBLIOGRAFIA

- Bermúdez Durana, J. A. (2011). *El futuro de la protección de datos personales en Colombia*. Colombia. Portafolio.
- Rojas Bejarano, M. (2014). *Evolución del derecho de protección de datos personales en Colombia respecto a estándares internaciones*. Bogotá, Colombia. Universidad Católica de Colombia.
- Soto Espinosa, C. C., y Ducuara Cuervo, C. A. (2018). *Protección de datos personales en los servicios de internet.* Bogotá, Colombia. Universidad Católica de Colombia.
- Forero Loaiza, D. C. y Vélez Trucco, S. (2016). *Ley 1581 de 2012: Contextualización de la norma a nivel nacional e internacional y análisis de algunas sanciones interpuestas*. Colombia. Universidad Pontifica Bolivariana.
- Mendoza Morales, J. A. (2015). *Protección de datos personales en Colombia.* Colombia. Universidad Militar Nueva Granada.
- Del Peso Navarro, E. (2000). *La protección de datos personales y la privacidad en internet.* Colombia.
- Corte Constitucional de Colombia. (16 de junio de 1992). *Sentencia T-414 de 1992.* M. P. Barón Ciro Angarita.
- Corte Constitucional de Colombia. (5 de septiembre de 2002). *Sentencia T-729 de 2002*. M. P. Eduardo Montealegre Lynett.
- Corte Constitucional de Colombia. (5 de noviembre de 1998). *Sentencia SU 642 de 1998*. M. P. Eduardo Cifuentes Muñoz.
- Corte Constitucional de Colombia. (26 de junio de 2002). *Sentencia C-489 de 2002*. M. P. Rodrigo Escobar Gil.
- Corte Constitucional de Colombia. (16 de octubre de 2008). *Sentencia C-1011 de 2008*. M. P. Jaime Córdoba Triviño.

- Corte Constitucional de Colombia. (6 de octubre de 2011). *Sentencia C-748 de 2011*. M. P. Jorge Ignacio Pretelt Chaljub.

- Congreso de la República de Colombia. (31 de diciembre de 2008). Ley 1266 de 2008. "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

- Congreso de la República de Colombia. (5 de enero de 2009). 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".

- Congreso de la República de Colombia. (17 de octubre de 2012). Ley 1581 de 2012. "Por la cual se dictan disposiciones generales para la protección de datos personales".

- Congreso de la República de Colombia. (6 de marzo de 2014). Ley 1712 de 2014. "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

- Presidencia de la República de Colombia de Colombia. (15 de mayo de 2009). Decreto 1727 de 2009. "Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información".

- Presidencia de la República de Colombia. (6 de agosto de 2010). Decreto 2952 de 2010. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008".

- Presidencia de la República de Colombia. (27 de junio de 2013). Decreto 1377 De 2013. "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".

- Presidencia de la República de Colombia. (13 de mayo de 2014). Decreto 886 de 2014. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos".

- Presidencia de la República de Colombia. (26 de mayo de 2015). Decreto 1074 de 2015. "Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo".
- Naciones Unidas. (10 de diciembre de 1948). *Declaración Universal de Derechos Humanos*.
- Naciones Unidas. (23 de marzo 1976). *Pacto Internacional de Derechos Civiles y Políticos*.
- Corte Interamericana de Derechos Humanos. (7 al 22 de noviembre de 1969). *Convención Americana de Derechos Humanos*.
- Asamblea Nacional Constituyente. (20 de julio de 1991). *Constitución Política de Colombia*.
- Superintendencia de Industria y Comercio. *Protección de datos personales.* Colombia.
- Superintendencia de Industria y Comercio. (2020). *Decisiones Administrativas.*
- Superintendencia de Industria y Comercio. (2021). *Decisiones Administrativas.*
- Superintendencia de Industria y Comercio. (2022). *Decisiones Administrativas.*