

**EFICACIA DE LA LEY 1581 DE 2012 SOBRE PROTECCIÓN DE DATOS
PERSONALES PARA GARANTIZAR EL DERECHO A LA INTIMIDAD.**

Por: Andrés David Muñoz Quiroz y Christian Andrés Díaz González

Asesor: Dany Steven Gómez Agudelo

Trabajo de grado para optar al título de Abogado

**UNIVERSIDAD CATÓLICA LUÍS AMIGÓ
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
MEDELLÍN**

2021

Tabla de contenido

Introducción.....	4
Capitulo I. Nociones generales del derecho a la intimidad y elementos estructurales del habeas data.....	8
Capitulo II. Mecanismos de protección existente en la Ley 1581 del 2012 para ofrecer límites a terceros que están encargados del tratamiento de datos personales, en el sector privado...21	
Conclusiones.....	29
Referencias	31

Resumen

Conforme avanza el esquema social y la tecnología, los datos personales adquieren un papel más relevante e indispensable en la interacción con la sociedad y sus entidades tanto privadas como públicas; por su parte, se empieza a percibir cómo la privacidad pierde la garantía de su cumplimiento, en aras de la protección nacional en algunos casos a causa de problemáticas como el terrorismo, control social y la aplicación de telemetría con fines comerciales, donde empresas y conglomerados económicos recopilan en bases de datos, información personal para analizar los gustos de los consumidores, situación de salud, núcleo familiar; situaciones que cuestionan sobre la importancia de la privacidad, cuando la política de los Estados cada vez más aceptan sin reparo, la implementación de sistemas de vigilancia, recolección de información sin consideración a los ciudadanos y cambiando la prevención por el control, otorgando vía a la intromisión de empresas privadas. Es indispensable el análisis del derecho a la intimidad como garantía constitucional, así como el método para su protección.

Palabras clave: Derecho fundamental, datos personales, garantía, habeas data, intimidad, privacidad.

Abstract

As the social scheme and technology advance, personal data acquires a more relevant and indispensable role in the interaction with society and its private and public entities; For its part, it is beginning to perceive how privacy loses its guarantee of compliance, for the sake of national protection in some cases due to problems such as terrorism, social control and the application of telemetry for commercial purposes, where companies and economic conglomerates they compile in databases, personal information to analyze consumer tastes, health situation, family nucleus; situations that question the importance of privacy, when the policies of the States increasingly

accept without hesitation, the implementation of surveillance systems, collection of information without regard to citizens and changing prevention for control, giving way to meddling by private companies. It is essential to analyze the right to privacy as a constitutional guarantee as well as the method for its protection.

Key words: Fundamental right, guarantee, habeas data, intimacy, privacy, personal information.

Introducción

En Colombia, la esfera social acogió del mismo modo que gran mayoría de países globalmente, la tecnología y los medios electrónicos como un sistema esencial en la interacción diaria con las demás personas, en el entorno laboral, académico, político, científico etc. Los adelantos en materia de datos personales en el siglo XXI, han repercutido como uno de los mayores avances hechos por la humanidad, refinándose en especial las bases virtuales, por otro lado, se han refinado las máquinas, su programación y la implementación de aplicaciones virtuales, para el beneficio determinado de algunas personas jurídicas o privadas con una relativa facilidad. Esta adopción reciente de la tecnología como elemento indispensable, ha dejado la puerta abierta a la inseguridad de nuestra información personal.

Aunque el tema de la seguridad informática no es tratado en esta investigación, está relacionado indirectamente, en algunas ocasiones al cometerse delitos informáticos, también se vulnera la privacidad y el Estado debe tomar las medidas necesarias para detener estas situaciones. Se observa que el mejoramiento en las técnicas y medios para lograr estos fines no solamente están inmersos en una determinada área del derecho, como por ejemplo la penal, que con la creación de la unidad especializada c4 en Bogotá ha fortalecido su estructura, sino además el resto de áreas tiende a mejorar y adaptarse frente los retos que plantea el entorno actual.

El objeto de esta investigación consiste en ahondar analíticamente lo concerniente a la vulneración del derecho a la intimidad por parte de entidades privadas, las cuales son las encargadas de regular la información personal de cada usuario. A lo largo de esta investigación se examinó, haciendo uso de técnicas de revisión documental, los antecedentes legislativos, jurisprudenciales, y actos jurídicos más relevantes frente a vulneraciones al derecho del habeas data en contraste con la eficacia de los mecanismos de protección que otorga la ley; retrospectivamente, se recolectaron elementos jurídicos de nuestra legislación colombiana y de la Superintendencia de Industria y Comercio, ente de control y máxima autoridad en estos asuntos; cuyos actos administrativos, resoluciones, órdenes y demás pronunciamientos, darán una muestra de cómo se ha visto reflejada la eficacia del Estado por medio de sanciones o acciones dirigidas a estas entidades privadas por el mal manejo y uso de esta información indebidamente, dado que estas son las encargadas de administrar información personal; a través de los mecanismos establecidos por la Ley 1581 del 2012. Dicha ley brindará una guía de cómo enfrentar esta problemática que se ha dilucidado por parte de entidades privadas que sin ningún tipo de rigurosidad en protocolos de seguridad, donde en ocasiones se ha violentado y vulnerado este derecho fundamental cuyo fin, en el contexto de esta investigación, es la protección de esa información confidencial y de mayor importancia, por parte de la persona encargada que suministra esta información.

El uso arbitrario de políticas plasmadas en términos y condiciones encaminadas a la regulación de la privacidad de los usuarios en el campo informático y su manipulación, es un tema contemporáneo que afecta diferentes esferas sociales, que reflejan la incapacidad del Estado a la hora de proteger el derecho a la privacidad y la información en bases de datos efectivamente; esto se evidenció con el aumento progresivo de infracciones por parte de los encargados del tratamiento de datos, así como la necesidad en Colombia de una regulación específica para evitar estos hechos que han afectado y siguen afectando a varias personas. Un primer objetivo es ahondar en el asunto concerniente a estas vulneraciones o abusos y encontrar bajo que lineamientos se podría hablar de una garantía real de protección a la privacidad; por ello es importante establecer la eficacia de los mecanismos legales establecidos en la Ley 1581 de 2012, para lograr una protección al derecho fundamental a la intimidad frente a terceros por medios electrónicos. Además de

buscar mecanismos inmersos en la misma que permitan lo anteriormente expuesto; un segundo objetivo es identificar a través de los mecanismos legales de protección en la ley 1581 de 2012, las sanciones aplicadas por la Superintendencia industria y Comercio, a terceros por el mal manejo del habeas data. Por último, definir los mecanismos de protección existentes en la Ley 1581 de 2012, para ofrecer límites a los terceros que están encargados del tratamiento de datos personales, en el sector privado, toda vez que se menciona bastante a los particulares, pero los Estados de manera más frecuente y minuciosamente promueven sistemas cuyo fin es aunar esfuerzos, en los sectores privado y público, en pro de sus beneficios.

Dado lo anterior, cabe preguntarse: ¿Cuál ha sido la eficacia de los mecanismos legales establecidos en la Ley 1581 de 2012, para lograr una protección al derecho fundamental a la intimidad frente a terceros por medios electrónicos?

Además, esta investigación tiene una finalidad informativa, analítica y focalizada a un asunto que es esencial en el día a día y es desconocido e inexplorado por la mayoría de colombianos sea por factores culturales, sociales o de otra índole, es de suma importancia recalcar el uso sano, proporcional y garantista de los datos personales de la ciudadanía que bajo ningún pretexto puede usarse con fines lucrativos o cooperativos por personas jurídicas y naturales de manera desmedida. Se cuestiona, por ejemplo, el almacenamiento de fotos privadas e íntimas en un dispositivo móvil que solamente es relevante para el titular del derecho y que solamente debería ser analizado por orden judicial pero que en su defecto terceros particulares con términos y condiciones dolosos pueden disponer a su arbitrio y beneficio desproporcionadamente. Un mayor conocimiento con base constitucional y legislativa permitiría la obtención de herramientas y parámetros que podrían tenerse en cuenta por los receptores de esta investigación y así evitar la violación de información personal, sea o no sea con permiso no se deben menospreciar las garantías planteadas en la carta magna.

Para llevar a cabo este trabajo, se aplicó una metodología de investigación del nivel cualitativo, socio jurídica e histórico hermenéutico, se aplicó como instrumento de recolección de información, la revisión documental que permitió cuestionar la eficacia de la mencionada ley por la reiteración constante y frecuente de estas conductas indebidas

por parte de los infractores, afectando negativamente el conglomerado social. En los siguientes capítulos se procederá a mostrar las premisas planteadas, siendo la primera sección enfocada a conceptos y nociones jurídicas de derechos primordiales que engloba el manejo de información personal, además se observarán actos administrativos cuya función es confrontar la realidad socio jurídica que se vive en el país, esto se logra con órdenes y sanciones a encargados del tratamiento de datos personales y otras acciones. Luego en el siguiente segmento se procederá a describir los mecanismos que otorga la ley estatutaria 1581 de 2012 y demás disposiciones legales a fin de proteger derechos fundamentales referentes a datos personales, dejando una conclusión final basada en una petición hecha al área de investigación de protección de datos personales a cargo de la Superintendencia de Industria y Comercio encaminada a responder la pregunta que fundamenta este trabajo, es decir si desde la promulgación de la ley estatutaria de habeas data, la misma ha sido eficaz dados sus objetivos, así como del material bibliográfico utilizado.

Capítulo I. Intimidad y habeas data como derecho para establecer límites a los terceros en el sector privado, que están encargados del tratamiento de datos personales.

En el artículo 15 de la Constitución Política Colombiana se establece lo siguiente: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre y el Estado debe respetarlos y hacerlos respetar” (Constitución, 1991, art. 15). Sin embargo, se encuentran con un panorama adverso puesto que la información de los ciudadanos, usuarios o contratantes no es tan respetada en la realidad y cada vez más se observan y normalizan conductas que vulneran la intimidad, sin reparo del respeto propicio con que se debe tratar este derecho.

De igual manera, la protección, tratamiento y violación de datos personales son temas muchas veces desconocidos o ignorados para algunas personas, estas suelen aceptar términos y condiciones de entidades privadas, de forma verbal, escrita o por conducta tácita de aceptación, sin siquiera darse cuenta de cuáles son las garantías referentes a este derecho fundamental plasmado en el artículo 15 de la C.N materializado en disposiciones normativas inmersas en la ley estatutaria 1581 de 2012 y la Ley 1266 de 2008, además de otras disposiciones legales que consolidan valor a la defensa prestada por este derecho. La adecuación de las empresas al generar políticas de privacidad que se ajustan a vacíos legales en normativas locales, es un problema sin solución aparente, el artículo 17 de la Ley 1581 de 2012 en su estructura establece los deberes a los responsables del tratamiento de los datos personales, se resaltan los de informar al titular el uso de la información proporcionada por el mismo y la garantía de protección adecuada, que cuando se vaya a proporcionar a terceros se avise y pida autorización, esto en la mayoría de casos no se materializa produciendo una afectación del derecho a la intimidad personal a consumidores y demás beneficiarios.

Adicionalmente, la información sensible de una persona fuera de un incidente judicial previamente reglado y justificado como en el caso de un delito puede y debe ser analizada, pero el panorama es contradictorio cuando empresas privadas sin necesidad de un juez constitucional o de garantías tienen acceso a dicha información con métodos invasivos de la privacidad, en resumen, no es lo mismo la seguridad estatal y la protección de bienes jurídicamente tutelados, a la aceptación de términos sobre privacidad que aparentan tener más poder, incluso que el mismo Estado. Lo anterior, suele observarse con empresas de telecomunicación usando telemetría, sin reparo de las legislaciones diferentes al país natal de las mismas, la telemetría es una tecnología que mide información direccionada a un operador de sistema específico, la emisión de los datos se hace por diferentes medios electromagnéticos como teléfonos, celulares, computadores y básicamente en comunicación inalámbrica. Según la RAE, uno de los significados de la palabra telemetría es: “Conjunto de técnicas para la medida a distancia de magnitudes físicas”. En Colombia, es reciente el conocimiento de estos asuntos y se han generado la creación de filtros proteccionistas más complejos o niveles de seguridad más severos relativos a la informática y tecnologías que implican el control de los datos personales, a su vez medidas paralelas se toman para progresar en la esfera jurídica frente a estos temas. Al respecto “una limitante para el sistema jurídico colombiano consiste en que, a pesar de contar en la actualidad nuestro ordenamiento jurídico con múltiples normatividades que regulan el nuevo campo de acción entre los particulares y la actividad estatal, todavía no existe una conciencia ni una cultura informática” (Remolina, 2012, p. 86).

Por consiguiente, en Colombia desde 1992, la Corte Constitucional reconoció el derecho a la intimidad para controlar su existencia con las menores injerencias exteriores, se puede hacer valer “erga omnes” es decir ante el Estado y los particulares; la sentencia de la corte constitucional C-640 de 2010 nos señala cinco principios base de este derecho:

Son cinco los principios que sustentan la protección del derecho a la intimidad. Ellos se clasifican y explican en los siguientes términos: El principio de libertad, según el cual, los datos personales de un individuo, sólo pueden ser registrados o divulgados con el consentimiento libre, previo, expreso o tácito del titular, a menos que el ordenamiento jurídico le imponga la obligación de relevar dicha información, en aras de cumplir un objetivo constitucionalmente legítimo. En este

contexto, la obtención y divulgación de datos personales, sin la previa autorización del titular o en ausencia de un claro y preciso mandato legal, se consideran ilícitas. El principio de finalidad, el cual se expresa en la exigencia de someter la recopilación y divulgación de datos, a la realización de una finalidad constitucionalmente legítima, lo que impide obligar a los ciudadanos a relevar datos íntimos su vida personal, sin un soporte en el Texto Constitucional que, por ejemplo, legitime la cesión de parte de su interioridad en beneficio de la comunidad. De conformidad con el principio de necesidad, la información personal que deba ser objeto de divulgación, se limita estrechamente a aquella que guarda relación de conexidad con la finalidad pretendida mediante su revelación. (Corte Constitucional, Sentencia C-640, 2010).

Conforme a lo mencionado anteriormente, el derecho a la intimidad se puede vulnerar por la circulación no autorizada de datos sensibles, los cuales son una categoría de datos personales, sobre el particular se afirma que consiste en:

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

En teoría estos datos deben tener un nivel alto de seguridad, pues la información de esta índole tiene un valor altísimo para su titular, tristemente de manera proporcional también tiene dicho valor en el mercado y adecuado al marco capitalista en el que se desenvuelve es común su venta, el alcance que tiene la libertad como parte elemental en la privacidad se ve opacada cuando los particulares ejercen acciones que vulneran de dichos datos, ignorando sus deberes y obligaciones plasmadas en la Ley 1581 de 2012. “Esta información se ha convertido en un bien permanentemente comercializado en el mercado nacional e internacional y en un insumo diario de los sistemas de información privados y gubernamentales” (Angarita, 2010, p. 492).

En este orden de ideas, el habeas data es un derecho que está inmerso en la mayoría de los marcos normativos en los que se desarrolla alrededor del mundo, si se realiza una consolidación de todos los aspectos que se encuentran en éste, para encontrar un equilibrio de funcionamiento, se tendrá en cuenta que son importantes tanto los intereses públicos como los privados y que estos, a su vez, sean comprometidos en la protección eficaz de la información que las personas suministran, primero realizando explicación del para que se recolectan estos datos y dando siempre la opción voluntaria de proveer o no la información, aportando en todo momento seguridad y confianza sobre el tratamiento de estos datos. A propósito la Unión Europea (2011), afirma:

Un marco sólido en materia de protección de datos también sirve a intereses públicos y privados más amplios en una sociedad de la información donde el tratamiento de datos se ha vuelto omnipresente. La protección de datos promueve la confianza y la confianza constituye a su vez un aspecto esencial del buen funcionamiento de una Sociedad (diario oficial de la Unión Europea, 2011, p. 3).

Como premisa sobre el habeas data en el contexto reciente y el ascendente poder informático que paulatinamente desafía los sistemas normativos establecidos en el ámbito jurídico, añadiendo fluctuaciones más severas a conceptos previos; sobre el tema la máxima autoridad constitucional expresa:

Surge como un cuerpo normativo singular orientado a proteger las libertades individuales. Dada la existencia extendida de bases de datos de carácter personal, magníficas condiciones de interconexión y accesibilidad, y posibilidades de uso en tiempo real, el habeas data es la respuesta del constitucionalismo para enfrentar las amenazas que el ejercicio inorgánico de este poder supone para la libertad de los seres humanos (C.const, SU-458, 2012).

Una característica permanente del derecho en general es su adaptabilidad a las necesidades sociales, aun así, Bejarano haciendo referencia al manejo de la información plantea la siguiente afirmación: “A pesar de que el uso y manejo de la información no es un tema nuevo en Colombia, se ha observado que las políticas definidas acerca de protección han resultado insuficientes, al exceder los medios de control y administrativos gubernamentales” (Bejarano, 2014, p. 109).

En este sentido, se genera un análisis comparativo o contraste con diferentes políticas

aplicables al asunto en cuestión alrededor del mundo que demuestran, qué si bien en nuestro país tenemos legislación aplicable, no es suficientemente efectiva ya que las políticas de privacidad, bases de datos e información, pueden ser vulneradas por delincuentes, los mismos creadores del documento virtual o en su defecto el software utilizado e inclusive los mismos usuarios al adherirse a dichas políticas, las cuales deben permitir que el usuario decida conscientemente, e informe como desea que sus datos sean usados con esta premisa, se aprecia un panorama de desigualdad entre las empresas y los usuarios respecto a el manejo de datos y se observa la imposibilidad de los usuarios para informarse lo que ocurre con el manejo de su información personal, cuya protección está basada en el mercado y la protección de datos expresada en contratos de propiedad con la información susceptible de ser comercializada con terceros.

Para hablar de la protección de datos personales es necesario hablar del fundamento normativo, el cual se ve evidenciado en la ley estatutaria 1581 de 2012 su finalidad es: “protegernos como individuos, y garantizar el derecho a conocer y autorizar que información personal está en determinada base de datos y derecho a autorizar o no el tratamiento de dichos datos personales”. (Garzón, 2015, p. 2). Esta ley, desarrolla y fundamenta lo que en el art 15 de la constitución política de Colombia se plantea garantizar y lo plasmado, el artículo reza:

“Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre. 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”.

Dicha normativa desarrolla el habeas data en especial su última parte. La corte hace mención concerniente al manejo de la información que le pueden dar las personas naturales; luego de creada la constitución política del año 91 sobre la privacidad e intimidad como: “la intimidad, contiene una zona de reserva para la propia persona, de la que quedan excluidos los demás, a menos que la persona protegida decida voluntariamente compartir dicho ámbito. Contiene dicho artículo, entre otros, los derechos a la intimidad personal y familiar, al buen nombre, al habeas data y a la inviolabilidad de la correspondencia y demás formas de comunicación privada. Todos estos derechos están unidos por su finalidad, la cual es aislar a la persona de las injerencias de terceros, así como proteger su imagen” (Corte Constitucional, T-412, 1992).

Desde este punto se comienza a desarrollar dicho concepto. La intimidad es un derecho enteramente ligado a la protección de datos personales ampliando más su significado se interpreta a su vez: “hace referencia al ámbito personalísimo de cada individuo o familia, es decir, a aquellos fenómenos, comportamientos, datos y situaciones que normalmente están sustraídos a la injerencia o al conocimiento de extraños” (Faceta jurídica, 2016, p.61).

Es entonces una parte esencial de la esfera privada del ser humano, a la cual ni el Estado ni los demás ciudadanos tienen derecho a acceder salvo algunas excepciones.

La información privada es aquella que se encuentra en el ámbito propio del sujeto concernido y, por ende, sólo puede accederse por orden de autoridad judicial competente y en ejercicio de sus funciones y por último, la información reservada, que es, aquella que sólo interesa al titular en razón a que está estrechamente relacionada con la protección de sus derechos a la dignidad humana, la intimidad y la libertad; como es el caso de los datos sobre la preferencia sexual de las personas, su credo ideológico o político, su información genética, sus hábitos (Corte Constitucional, Sentencia C1011, 2008).

Este apartado refuerza lo pregonado, ninguna persona, entidad o individuo ajeno, puede obtener ningún tipo de información privada perteneciente a una persona en particular, con la excepción de que el solicitante sea el mismo titular o también, por ejemplo, alguna orden de tipo judicial, con el fin de obtener datos sobre documentación privada, información necesaria para procesos penales o simplemente libros comerciales; esta información en cualquiera de los casos siempre tiene que ir ligada a la protección de los derechos y velar primordialmente por la dignidad del individuo o los individuos implicados, normalmente familiares.

Posterior a la promulgación de la Constitución Política, surge otra línea de definición por parte de la Corte Constitucional en otra sentencia desarrollando la intimidad en el campo de datos personales y su afinidad con otras disposiciones expone que es: “una manifestación del derecho fundamental al libre desarrollo de la personalidad” (Corte Constitucional, T 340, 1993).

En el ámbito internacional, mucho antes que la ley motivo de esta investigación, ya existían antecedentes planteados sobre este importante concepto:

La recopilación y el registro de información personal en computadoras, bancos de

datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley. Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y porque nunca se la utilice para fines incompatibles con el Pacto. (Comité de los Derechos Humanos, Observación General No. 16 Artículo 17, #10,1988.).

Se trae a colación esta citación ya que, es relevante la influencia del Estado como garante de los derechos de los habitantes, en este caso exclusivo, de la vida privada de los mismos; incluyendo planes o medidas preventivas y eficaces para cada uno de ellos ya que su fin siempre será velar por la seguridad con hechos fundamentados en las leyes. Así mismo, fue en el contexto internacional que se empezó a construir, materializar y consagrar, la defensa de la intimidad a niveles continentales.

A través del decreto 1377 de 2013 se reglamentan algunos aspectos de la ley 1581, en aras de una mejor aplicación en el entorno jurídico, además de ampliar el concepto de elementos fundamentales como la aclaración sobre tipología de datos personales. Por ejemplo, los datos sensibles, esto es, “aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación” (Decreto 1377, 2013, art 3). Este acápite establece claridad sobre dichos datos y enuncia algunos de los mismos como lo son: origen racial, orientación política y sexual, datos biométricos entre otros. Se puede afirmar que los datos sensibles son los que se pretenden salvaguardar con estas expresiones legislativas el artículo 2 ibídem reza :

“Se exceptúan de la aplicación de dicha Ley y del presente Decreto, las bases de datos mantenidas en un ámbito exclusivamente personal o doméstico. El ámbito personal o doméstico comprende aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales” (Decreto 1377, 2013, art 2).

Cuando una persona realiza algún procedimiento donde se ve inmersa su información personal, está dejando su identidad a la deriva, y es en parte su responsabilidad estar al tanto de lo que ocurre, por ende, muchas veces resulta inevitable el compromiso de esta tipología de datos. En situaciones donde se vulneran los datos de uso personal o doméstico, la dirección apropiada o la acción a seguir es la tutela; no se aplicará este

reglamento.

En el caso de las fotografías depende la finalidad de las mismas, por ejemplo, si tiene o no fines comerciales. Además, en términos generales no todas las fotos contienen datos personales estos factores dependen de vestimentas, partes del cuerpo identificables, el uso o no de elementos que cubran el rostro entre otros. “La foto será Dato Personal en la medida en que permita establecer la identidad de una o varias personas naturales en particular” (Sic, 2020, Guía sobre el tratamiento de datos personales en fotos, p. 8).

Hay circunstancias en que se distingue una persona por características únicas de estas, por ejemplo, un tatuaje, una marca de nacimiento, partes corporales o comportamientos. Este conjunto de elementos hacen parte de los datos biométricos su vez, estos permiten la identificación de las personas por lo tanto pueden y deben ser protegidos “quien toma una fotografía a personas naturales determinadas o determinables está recolectando y tratando Datos Personales. Razón suficiente para cumplir las normas señaladas y usar las fotos únicamente para los fines autorizados por el Titular del dato o por la ley” (Sic, 2020, Guía sobre el tratamiento de datos personales en fotos, p. 9).

Cuando los datos sensibles pertenecen a un menor de edad, el responsable y tratante de sus datos, debe tener más atención sobre estos y velar por los derechos fundamentales de los menores, toda vez que la familia, la sociedad y el Estado tienen la obligación de asistir y proteger al niño para garantizar su desarrollo armónico e integral y el ejercicio pleno de sus derechos.

Si se pretende hacer uso de los datos en mención es esencial que se garanticen primero el respeto por el último inciso del artículo 44 y que se asegure, que no habrá vulneraciones a sus derechos fundamentales ni se pueden poner en riesgo. “En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes”. (Ley 1581, 2012, art 7).

En las sociedades actuales no se concibe que las personas no hagan uso de elementos electrónicos, por el contrario, es cada vez más promovido su uso, como es apreciable en la realidad.

No hay menor de edad que no disponga de algún dispositivo que le permita conectarse a la red, ya sea una tablet, ordenador o móvil, asimismo, suelen navegar a través de ellos de forma totalmente despreocupada, aportando datos personales como de su entorno familiar y círculo de amistades, en algunas ocasiones

especialmente sensibles, sin percatarse de quien puede estar recibiendo esa información y cómo la va a utilizar. (Berrocal, 2016, p. 13).

Las sociedades actuales dependen profusamente de las nuevas tecnologías (NT) lo que conlleva a una evolución social, cultural y jurídica. “hoy las instituciones jurídicas y los derechos fundamentales de los ciudadanos son de una sociedad donde las NT y las TIC y, en especial, la red, han devenido el símbolo emblemático de nuestra cultura, también de nuestra cultura jurídica” (Pérez, 2017, p. 36).

El escenario adquiere complejidad en situaciones donde las empresas conocen de primera mano el contenido de estos datos, cuya intromisión es aceptada usualmente sin reproche, al no haber claridad sobre su uso por parte de las empresas o en su defecto por ignorancia del propio usuario, que en ocasiones a causa de falta de interés, de tiempo u otra variable no presta atención sobre la aceptación que hace, sea de manera verbal, escrita o con acciones inequívocas; el uso de las redes sociales y la divulgación de muchos datos que estas plataformas almacenan, pueden generar un riesgo para el ciudadano, “el mundo digital ha evolucionado para permitir a las personas realizar una gran cantidad de actividades sin tener que desplazarse a diferentes lugares, sin embargo, para que la experiencia sea cada vez más satisfactoria, es necesario que el usuario deposite sus datos personales en la web, lo cual tiene múltiples consecuencias (Obando, 2020, p. 19)’’.

La comercialización de datos personales, por ende, es una realidad palpable que amplía también el espectro de acción del habeas data, así como el de las autoridades que vigilan el cumplimiento de los lineamientos legales por parte de terceros o encargados de estos.

Así mismo, señala Solevé (2000) que “las políticas de manejo de información y de privacidad que proveen las empresas resultan muy ambiciosas y poco efectivas en la realidad” (p. 1451), no les permite a los usuarios tener poder de decisión, lo cual implica que se pierde de vista el verdadero origen del problema que reviste la privacidad en el ciberespacio, esto es, la desigualdad entre los usuarios y las compañías que manejan los datos. A esto se le suma el constante valor económico que se le ha otorgado a los datos personales en el mercado nacional e internacional. Un ejemplo claro son las ya conocidas técnicas de rastreo denominadas “cookies”; entre sus funciones permiten recolectar información en tiempo real sobre cómo actúan las personas en internet, es decir, cuáles son las páginas que visitan, los contenidos que consumen, la hora, fecha y lugar de las

actividades, la frecuencia de las visitas, qué compran en línea, entre otros.

En el caso de las “cookies” se hace aplicación de la ley 1581 de 2012 por el tipo de datos que representan en nuestra legislación, como lo dejaba claro la Corte: “De ahí que uno de los grandes retos de la protección de los datos personales es la creación de mecanismos para hacer responsables a los particulares por el tratamiento inadecuado y abusivo de datos personales” (Corte Constitucional, C-748-2011, p. 141).

Partiendo del anterior antecedente, este reto se materializó en tan solo un año consecutivo. Haciendo uso de la interpretación inmersa en el parágrafo del artículo 2 sobre el ámbito de aplicación, “los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo” (Ley 1581, 2012).

Se termina concluyendo que las técnicas de recolección informáticas no están específicamente reguladas, pero son amparadas por la ley, en caso de vulneraciones, aunque generan inconvenientes al estar manejadas comúnmente por empresas extranjeras con servidores en otros países lo que dificulta una eficaz y pronta protección en caso de una vulneración.

Recientemente, se ha producido una problemática con aplicaciones generalmente de empresas privadas foráneas y nacionales, las cuales se convierten en un amplio medio de difusión entre la sociedad colombiana y que a su vez implementan cookies que recolectan datos sensibles, la incertidumbre se da en el momento que no hay claridad sobre el uso de dichas recolecciones y dudosas políticas de manejo frente a ellos, “una cookie es un mecanismo que se instala en los equipos o dispositivos (bien sea celular, computador portátil, u otro) de las personas residentes o domiciliadas en la República de Colombia con el objetivo de recolectar algunos de sus Datos Personales (Sic, resolución número 53593,2020).

En la anterior diligencia mencionada, surgió un conflicto con la empresa Google y sus filiales, así como YouTube, aplicación que también le pertenece. Entre las conclusiones más importantes se encuentran las siguientes:

GOOGLE LLC recolecta la siguiente información personal: nombres; contraseñas; información de pago; números de teléfono; edad; dirección de correo electrónico; medios de pago; contactos; gustos y preferencias; dirección IP; localización; datos de sensores del dispositivo; puntos de acceso WI-Fi; torres de telefonía y

dispositivos con Bluetooth activado; términos de búsqueda; vistas e interacciones con videos; contenido y anuncios; información sobre la voz y el audio; videos mirados; compras; personas con las que se comunica o comparte contenido; actividad en sitios y aplicaciones de terceros; historial de navegación; identificadores únicos; tipo y configuración del navegador; tipo y configuración del dispositivo; sistema operativo; información sobre la red móvil; como el nombre y número de teléfono del proveedor; y el número de versión de la aplicación (Sic, resolución, numero 53593,2020).

Se entiende por esto que básicamente esta empresa tiene acceso a la mayoría de datos personales que puede manejar un ser humano en la actualidad, máxime cuando hay una dependencia directa con la forma como está construida la sociedad colombiana, la cual dispone de sistemas provechosos utilizando medios tecnológicos, siendo el más elemental los computadores fijos o portátiles, además de los teléfonos móviles inteligentes; sin mencionar la cantidad desbordada de aplicaciones generadas paulatinamente cuyos objetivos son variados acorde a los lineamientos del mercado y la demanda social.

Es entendible que las alternativas actuales apliquen estrategias comerciales, adaptados al mundo moderno, el verdadero problema es que las políticas de privacidad y la cantidad absurda de permisos que requieren los servicios para ser usados correctamente por los usuarios no están cobijados 100% a la luz de la ley estatutaria.

Los resultados de la evaluación inmersa sobre la política de privacidad de Google, en concordancia con lo establecido con la ley 1581 de 2012 son los siguientes:

i. Número de ítems evaluados: 19 ii. Número de obligaciones que se cumplen correctamente: 4 (21,05%) iii. Número de obligaciones que se cumplen parcialmente (P): 5 (26,31%) iv. Número de obligaciones que no se cumplen: 10(52,63%) (Sic, resolución, numero 53593,2020, p. 25).

Al final, se termina concluyendo con un conjunto de ordenes encaminadas a la optimización e implementación de una política de privacidad sólida, adecuada a la legislación nacional, que permita a los usuario en especial a los menores de edad, tener pleno conocimiento sobre el tipo de uso que harán las empresas y terceros con sus datos personales, un avance de peso considerando que GOOGLE LLC posee y trata datos personales de 1,847,592 niños, niñas y/o adolescentes y 38,962,184 personas mayores de

edad domiciliadas o residentes en la República de Colombia.

Otro caso apreciable ocurrió con TikTok, esta aplicación convertida en viral por su rápida expansión administrada por la empresa Byte Dancé ltd, de origen chino conforme a la información otorgada por la organización “TikTok tiene 12,447,549 cuentas registradas por ciudadanos o residentes en Colombia. De aquellas, 1,933,835 cuentas son de usuarios menores de 18 años” (Sic ,2020, resolución número 62132, p.7).

A raíz de la controversia se logró conseguir información importante sobre cómo se estaban manejando los datos de estas personas, arrojando datos alarmantes por las implicaciones jurídicas que tienen, para obtener dicha información se utilizaron medios propios de la autoridad administrativa, en el caso concreto se hizo revisión de las políticas de privacidad en la aplicación llegando a la siguiente conclusión entre otras. Los resultados de la evaluación son los siguientes. Número de ítems evaluados: 24. ii. Número de obligaciones que se cumplen correctamente: 6(25%). iii. Número de obligaciones que se cumplen parcialmente (P): 4(16,67%). iv. Número de obligaciones que no se cumplen: 14(58,33%)”. (Sic, 2020, resolución número 62132).

El enfoque de los componentes o ítems era sobre el deber de informar al titular de los datos al momento de solicitar la autorización concerniente a la aceptación de las políticas de privacidad manejadas por la aplicación.

Entre las múltiples medidas obligatorias tomadas contra Tik tok, están la orden a de implementar procedimientos más rigurosos a la hora de informar claramente que tipos de normativas están aceptando; al lado de una redacción en castellano puesto que la original estaba en idioma chino. De forma similar sobre los menores que hacen uso de la aplicación la orden estuvo dirigida a que “ implementen un mecanismo o procedimiento apropiado, efectivo y demostrable para dar cumplimiento a los requisitos especiales que ordena el artículo 12 del Decreto 1377, para la recolección y Tratamiento de los datos personales de niños, niñas y adolescentes (Sic, 2020, resolución número 62132).

En sentencia C -478 de 2011, la Corte Constitucional emite otro punto de interpretación sobre el alcance de este derecho el cual está vigente hasta el día de hoy “se entiende el habeas data como un derecho fundamental autónomo, el núcleo esencial del derecho”, entendiéndose esto como la auto determinación informática y libertad incluida la libertad

económica por lo cual se hace necesario por parte del Estado crear mecanismos que no se limiten solo al ámbito jurídico. Encima también engloba unos principios que sirven de base a este derecho y le aporta una naturaleza más cautelara, máxime en el caso donde hay manejo de terceros de datos personales exceptuando los de dominio público.

El principio de finalidad supone la existencia de un objetivo constitucional legítimo que, a su vez, delimita qué puede hacerse con el dato. Por su parte, el principio de necesidad se refiere a que el tratamiento de dicho dato cumpla con el fin que abarca su manejo. Por último, el principio de circulación restringida, conduce a que el flujo de la información deba tener relación directa con la finalidad, al tiempo que restringe el acceso masivo a la información, con excepción de los datos de naturaleza pública (Corte Const, T-020, 2014).

Consecuencialmente al avance jurídico, social y tecnológico del país, se puede concluir que hay falencias por parte del Estado y algunas empresas privadas que impiden garantizar la adecuada protección al derecho a la intimidad de los ciudadanos y usuarios.

Un estudio de la Superintendencia de Industria y Comercio sobre medidas de seguridad en el tratamiento de datos personales hecho en noviembre 22 de 2019, concluye hallazgos interesantes sobre este asunto, con base en información suministrada por 32,763 organizaciones Responsables del Tratamiento de datos que registraron sus bases de datos en esta Entidad, desde el año 2015 hasta el 18 de septiembre de 2019. De éstas, 31.410 son empresas privadas (95.8%) y 1.353 entidades públicas (4,1%). Las tres conclusiones más relevantes para esta investigación son:

1.65,5% de las empresas y las entidades públicas no han implementado medidas apropiadas y efectivas para garantizar la seguridad de los datos personales.

2.El 79% de las organizaciones no han implementado una política específica que regule el acceso a la información personal de las bases de datos con información sensible.

3.El 88% de las entidades no han puesto en marcha una política de protección para el acceso remoto a la información personal, y el 83% tampoco cuenta con un procedimiento implementado de auditoría de los sistemas de información que contengan datos personales.

Este estudio se hizo por medio de un formulario del RNBD(Registro Nacional de Bases de Datos) a cargo de la Sic.

El escenario es desalentador ya que denota una falta de responsabilidad en el manejo y

protección de base de datos por parte mayoritariamente de empresas privadas, además de falencias a la hora de garantizar a los ciudadanos un uso adecuado de su información, existiendo cantidad de sanciones con la misión de aminorar estos hechos, más hay dificultad en lograr la no repetición de conductas vulnerantes.

Pongamos por caso lo sucedido con LINIO DE COLOMBIA una empresa que fue sancionada en reiteradas ocasiones haciendo caso omiso a sus obligaciones legales como administrador de datos personales. La Sic arguyó sobre su decisión:

No puede convertirse en práctica empresarial que el titular del dato tenga que insistir en varias veces para que se garantice el respecto de sus derechos. Con una sola solicitud es suficiente y le corresponde al Responsable hacer efectivo el derecho de las personas dentro de los plazos máximos legales establecidos en la ley. Los derechos de los titulares son para respetarlos en el tratamiento de datos personales y no para dilatar su cumplimiento o negar su efectividad en la práctica (Superintendencia de industria y comercio, resolución 83882, 2018, p. 11).

Al contrario de lo buscado con las multas y sanciones pareciera de cierto modo que el capital de las empresas es tan grande, que terminan produciendo un resultado casi irrisorio en la funcionalidad de sus deberes volviendo en algún momento a recaer en una vulneración de derechos sin reparo del agravante por reiteración. La reincidencia en la comisión de la infracción (Ley 1581, 2012, art 24).

Las consecuencias del mal manejo de bases de datos son varias y con distintos niveles de afectación, vulneración de derechos en mayor o menor nivel como hemos advertido anteriormente por ello, es necesario conocer de qué forma se pueden amparar.

Capítulo II. Mecanismos de protección existente en la Ley 1581 del 2012 para ofrecer límites a terceros que están encargados del tratamiento de datos personales, en el sector privado.

Este acápite consiste en ahondar en lo concerniente a las herramientas jurídicas que otorga la ley frente a vulneraciones o abusos del derecho a la intimidad y encontrar bajo que lineamientos las entidades que producen este tipo de transgresiones a dicho derecho; se

sancionan, materializando, una garantía real de protección a la privacidad, además de buscar mecanismos que permitan lo anteriormente expuesto, este objetivo nos conllevará a dar una idea general de cómo estos mecanismos existentes establecidos por la ley 1581 del 2012, podrán dar una solución viable a aquellas personas titulares de la información soportadas en las bases de datos de entidades privadas, las cuales son las encargadas del manejo de la información personal otorgada por los contratantes.

En observancia a estos mecanismos en aras de darle una valoración adecuada al manejo de datos personales encontramos tres mecanismos, el primero está consagrado en el artículo 14 de la Ley 1581 del 2012 es la consulta, donde desde un principio se aprecia la importancia que le otorga la ley a estos procedimientos con la premisa “Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado” (Ley 1581, 2012, art. 14).

Se entiende entonces que el legislador dotó de tal relevancia estos mecanismos, que su accionar no es solo capacidad del titular del derecho sino también sus personas más cercanas (Causa habientes); Y es que el derecho fundamental a la intimidad, no solo es personal sino también familiar, esto cobra más sentido si se dimensiona como son las viviendas familiares actuales cuyo acceso a herramientas tecnológicas que permitan la comunicación es prácticamente imprescindible, las relaciones sociales por medios electromagnéticos como la telefonía móvil son ahora esenciales, y lo común es que una misma familia tenga conexión en un mismo dispositivo de telecomunicación o proveedor de internet. Siendo por ende la vulneración a la privacidad de un miembro de la familia traspasada casi que por mitosis al resto de integrantes. Además, se resalta la responsabilidad que tiene del responsable del tratamiento de estos datos de otorgar la información de manera oportuna, evitando dilaciones.

Frente al trámite de consulta es menester indicar que el titular o sus causahabientes (en caso de muerte del primero) podrán consultar de forma gratuita los datos personales del fallecido, al menos una vez cada mes en el calendario, y cada vez que existan modificaciones sustanciales de las Políticas de Tratamiento de la información que motiven nuevas consultas.

En este orden de ideas, cuando su periodicidad sea mayor a una por cada mes calendario, el responsable sólo podrá cobrar al titular los gastos de envío, reproducción y, en su caso, la certificación de documentos.

Por otro lado, el artículo 14 del estatuto 1581 de 2012 establece el término de diez días hábiles, una vez recibida la consulta para otorgar una solución, si no se puede cumplir con la obligación legal en ese término, se tendrán otros cinco días hábiles siempre y cuando se le indique al titular las razones de la demora y que sea justificable el atraso. (Rodríguez & Jaller, 2014, p. 86).

En consecuencia de lo anterior, se puede argumentar y tomar como ejemplo este caso en especial en cuanto al mecanismo de consulta, al presentarse el deceso del titular, ya que aún se puede hacer valer el derecho a la consulta de los datos personales de forma gratuita, y solamente si requiere algún tipo de envío, será cobrada; de no ser habilitado un tiempo por alguna circunstancia personal o situación externa, se dispondrá de 15 días hábiles para solucionar la consulta, diez días primero y después otros cinco días; tiempo que es avalado en cuanto se explique la causa del incumplimiento pactado con antelación. De no haber motivación que justifique la demora en responder por parte de la autoridad o causa excepcional, se aplicará la sanción correspondiente en estos casos: “Salvo norma legal especial y so pena de sanción disciplinaria, toda petición deberá resolverse dentro de los quince (15) días siguientes a su recepción” (Ley 1437, 2011, Art 14).

La figura de la consulta se desarrolló primero conceptualmente junto al reclamo en la ley 1266 de 2008, con el fin de ser un medio o mecanismo de protección al habeas data enfocado a personas jurídicas y naturales, pero haciendo hincapié en que el ámbito de acción era principalmente el comercial y crediticio, esto se esclarece en su preámbulo.

“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” (Ley 1266, 2008, preámbulo).

La sucesora ley de tratamiento de datos estaría formulada e impregnada de un carácter más proteccionista y general siendo elaborada en favor de las personas naturales junto a sus inherentes datos sensibles. Ambas siguen vigentes, pero se aplican acorde al contexto o pretensión jurídica respectivamente.

El segundo mecanismo planteado en la ley 1581 del 2012 es el reclamo. Dicho mecanismo tiene una finalidad que propende principalmente en hacer uso de un conjunto de acciones

que pueden ejercer los titulares de la información. Este mecanismo está definido en el artículo de la ley en mención; de la siguiente forma:

El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento (Ley 1581, 2012, art 15).

Cabe resaltar que de ambas herramientas otorgadas por el legislador sobre el habeas data, este elemento junto a la consulta y la queja plantean un requisito de procedibilidad que precede a la tutela en caso de una negativa por parte de la entidad a la cual se le interponga la petición modificatoria; y adquiere un carácter más riguroso que la mera consulta al involucrar términos temporales menores y más desarrollo jurídico.

Es de esta forma que el buen nombre junto a la autodeterminación informática son derechos fundamentales inseparables involucrados en el amparo constitucional y legal del concepto de habeas data como lo plantea la Corte constitucional:

El núcleo esencial del habeas data está integrado por el derecho a la autodeterminación informática y por la libertad, en general. La autodeterminación informática es la facultad que tienen las personas a las cuales se refieren los datos, de autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales (Corte Constitucional, T 657, 2005).

Como soporte a lo anterior la revista Faceta jurídica genera conclusiones y un planteamiento bastante asertivo sobre la autonomía del habeas data, pero también de su importancia y resalta aún más que pese a lo anteriormente mencionado, es un derecho que engloba y se constituye de muchos principios:

El reconocimiento del derecho fundamental autónomo al habeas data, busca la protección de los datos personales en un universo globalizado en el que el poder informático es creciente. Esta protección responde a la importancia que tales datos revisten para la garantía de otros derechos como la intimidad, el buen nombre, el libre desarrollo de la personalidad (Leyer, Faceta jurídica numero 65 Septiembre y Octubre de 2014).

Así mismo, con el fin de que la información corresponda a su realidad, el titular tendrá el derecho de solicitar la actualización, rectificación y supresión de dicha información. “Así lo estableció el artículo 21 de la Ley 1581 de 2012. Para lo cual, este deberá acatar las medidas correspondientes que se hayan destinado para tal procedimiento”. (Castañeda, 2018, p.34).

De acuerdo a lo anterior, se puede destacar que el autor apoya la idea y hace énfasis en algunas de las generalidades que tiene el titular, lo cual concuerda con lo expuesto en el artículo; ya que de este, sintetizamos que la actualización, supresión y rectificación son especificidades inmersas en el mecanismo de reclamo y las cuales se pueden utilizar en algunas de las situaciones en que se requiera hacer una modificación en la información personal; después de ser presentada de manera adecuada y pertinente no podrá ser removida o descatada ya que se estima como un derecho del titular y se encuentra respaldada por la legislación.

Ambos mecanismos mencionados tienen una relación directa con otro derecho fundamental afín al habeas data “los mecanismos de consultas y reclamos frente a los Responsables y Encargados del Tratamiento, constituye un desarrollo del artículo 23 de la Constitución Política, es decir, la reglamentación del derecho de petición frente a particulares que va específicamente orientado a la salvaguarda del derecho de habeas data” (SIC, resolución número 44019, 2020, p. 10).

Por otra parte, falta añadir que en años recientes, las empresas de telecomunicación privadas se han visto involucradas en la afectación de este derecho con argucias utilizadas en algunas ocasiones buscando el otorgamiento de un consentimiento o la aceptación de políticas de privacidad, han sido constantes, a su vez la reiteración de sus actuaciones contrarias a lo establecido legalmente. En estos casos la petición se enmarca bajo los parámetros de la ley 1755 de 2015 al añadir reglamentación dirigida a responsables y encargados de la información. “Toda persona podrá ejercer el derecho de petición para garantizar sus derechos fundamentales ante organizaciones privadas con o sin personería jurídica, tales como sociedades, corporaciones, fundaciones, asociaciones, organizaciones religiosas, cooperativas, instituciones financieras o clubes”. (Ley1755, 2015, art 32).

El régimen de la ley estatutaria de habeas data rige pues a las entidades privadas y modifica el trato de estas con los usuarios, generando una presión explícita encaminada al respeto de las garantías legales, aplicando nociones de equilibrio en una conexión que ya

es de por si inestable. Por el contrario, si en algún caso la problemática jurídica involucra una entidad pública se omite la competencia de la SIC por factor objetivo, siendo un asunto de otro organismo público, para esta situación. “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” (Ley 1581, 2012, art 23).

Al lado de los anteriores mecanismos se encuentra el más importante, la queja, no literalmente puesto que no se pone en duda la relevancia jurídica de los mencionados; sino que adquiere un mayor decoro al ser el último recurso posible de la ley 1581 de 2012 y es presentado ante la máxima autoridad en esta área, es decir, la Superintendencia de Industria y Comercio. Se menciona en dicha ley así: “El Titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio(SIC) una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento”. (Ley 1581, 2012, art. 16).

La reclamación previa a la queja, debe narrar claramente los hechos y declarar una pretensión relativa a los supuestos datos personales vulnerados o el manejo dado por la empresa a la que vaya dirigida. Los contenidos de la queja someramente son: ‘Nombre completo e identificación de la persona natural o jurídica contra la cual se dirige la denuncia, relato completo y legible de los hechos, copia de los documentos que respaldan la denuncia, manifestación clara de las pretensiones’” SIC, Tramites y servicios,2020.Si se presenta por una persona jurídica debe agregarse constancia del representante legal y en caso de que un apoderado la presente, adjuntará a la documentación su poder para llevar a cabo el acto jurídico.

En relación con lo expuesto el legislador dotó a la SIC de una capacidad sancionatoria manifestada jurídicamente por resoluciones efectuadas por este órgano, siendo un suplemento de la Ley 1266 de 2008 en aras de una estructura más compleja que permitiera cumplir más eficientemente con los objetivos de la entidad junto a sus funcionarios.

De ahí que la SIC establezca:

“ Una vez haya agotado el trámite señalado puede presentar la queja ante la Dirección de investigaciones de Protección de datos personales de esta

Superintendencia aportando las pruebas que pretenda hacer valer y de la reclamación correspondiente.” (Concepto n° 276941, Superintendencia Industria y Comercio, 2013).

Adicionalmente una de las funciones esenciales de la Dirección de investigaciones está señalada en el Decreto 4886 de 2011 en su primer acápite que reza: “Ejercer la vigilancia de los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países de la misma naturaleza, en cuanto se refiere a la actividad de administración de datos personales, en los términos de la ley”. Decreto 4886, 2011, Art 17.

Con el fin de estructurar sus funciones, el legislador exhorta la creación del Registro Nacional de Bases de Datos orden inmersa en el artículo 25 de la ley 1581 de 2012.”El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país”. A su vez el Decreto 886 de 2014 reglamento el marco por el cual funciona; asigna además a la Sic como autoridad del referido. Ha sido un avance consistente en la materia ya que permite un acceso público a la ciudadanía y demás interesados con una información precisa de quien o quienes son los responsables o encargados del tratamiento de sus datos, requisitos mínimos, tales como:

“1. Datos de identificación, ubicación y contacto del responsable del Tratamiento de la base de datos; 2. Datos de identificación, ubicación y contacto del o de los Encargados del Tratamiento de la base de datos; 3. Canales para que los titulares ejerzan sus derechos; 4. Nombre y finalidad de la base de datos; 5. Forma de Tratamiento de la base de datos (manual y/o automatizada), y 6. Política de Tratamiento de la información” (Decreto 886, 2014, art 5).

Permitiendo así agregar más herramientas garantes encaminadas a cumplir lo dispuesto en la ley con el objetivo del amparo legal en contrapeso a políticas de privacidad contrarias a lo establecido.

Con relación al último mecanismo, la acción de tutela; aunque no se indique explícitamente como tal, se conoce que hace parte del rango constitucional que inspira la legislación colombiana, siendo también el caso lógicamente de la ley 1581 de 2012. Al tener un carácter de ley estatutaria esta armonizada con los preceptos de la carta magna y tiene gran influencia garantista de nociones aplicadas por la Comisión Europea.

Sin perjuicio del ejercicio de la acción de tutela para amparar el derecho

fundamental del hábeas data, en caso que el titular no se encuentre satisfecho con la respuesta a la petición, podrá recurrir al proceso judicial correspondiente dentro de los términos legales pertinentes para debatir lo relacionado con la obligación reportada como incumplida (Ley 1266 de 2008, Art 16 II N.6)

Entre sus cualidades la tutela tiene las siguientes:

La acción de tutela, regulada en el artículo 86 de la C.P., se caracteriza por su probada eficacia para defender la efectividad de los derechos fundamentales. La revisión eventual de las sentencias que se profieran, por parte de la Corte Constitucional, de otro lado, ha permitido que progresivamente se conforme un cuerpo doctrinal que orienta la actividad judicial y que está atenta a adaptar los fallos a los nuevos retos y desafíos que enfrentan los derechos (Cifuentes, 1997, p. 128).

Además, se sustrae del artículo 86 que: “la protección inmediata de los derechos constitucionales fundamentales cuando quieren que estos resulten vulnerados o amenazados por la acción u omisión de cualquier autoridad pública o privada” (Const, 1991, art 86), de lo anterior, se puede afirmar que si en algún momento se prevé o se confirma algún tipo de incumplimiento a cargo del responsable de proteger la información del ciudadano, la acción de tutela va a ser la opción más viable después de haber utilizado alguna de las herramientas otorgadas, estableciendo su esencia subsidiaria cuando ya existen medios de defensa que amparen el derecho vulnerado.

Con el fin de acudir a esta acción, se deben tener en cuenta las condiciones especiales consideradas por la corte constitucional, siendo de vital importancia las primeras dos.

”(i) que la cuestión sea de relevancia constitucional; (ii) que se hayan agotado todos los medios de defensa judicial al alcance; (iii) que se cumpla el principio de inmediatez; (iv) si se trata de una irregularidad procesal, que la misma sea decisiva en el proceso; (v) que se identifiquen, de manera razonable, los hechos que generaron la vulneración de derechos fundamentales y (vi) que no se trate de una tutela contra tutela.” (C.const,T-034,2018).

Para concluir, la tutela será el medio más eficaz y el último recurso a aplicar luego de la negativa no justificada ante alguna solicitud, reclamo o queja planteada por el ciudadano ante la autoridad competente previo agotamiento de los elementos sobre información personal y cuyo mecanismo en la ley 1581 de 2012, haya sido deficiente en su función primordial; con la finalidad de no congestionar el sistema judicial, evitar la temeridad en

la acción de tutela y seguir el conducto regular.

En aras de materializar las funciones establecidas en la ley y la constitución, en efecto la SIC goza de diversas medidas tendientes a garantizar la realización de las disposiciones de la ley estatutaria 1581 de 2012, entre estas, las sanciones, las multas y suspensión de las actividades del banco de datos, esto ocurre así: “una vez establecido el incumplimiento de las normas de la presente normatividad por parte del responsable o el encargado del tratamiento, quién adoptará las medidas o impondrá las sanciones correspondientes” (Ley 1581, 2012, art 22). Las medidas que tome la autoridad deben ser objetivas, proporcionales al daño causado, cobijadas bajo unos criterios como el beneficio económico de los infractores, la negativa u obstrucción, etc.

Conclusiones.

En este trabajo de investigación se obtuvo información de la Superintendencia Industria y Comercio, específicamente al área de investigación de datos personales sobre la pregunta inicial de esta investigación y objetivo general. ¿cuál ha sido la eficacia de los mecanismos legales establecidos en la Ley 1581 de 2012, para lograr una protección al derecho fundamental a la intimidad frente a terceros por medios electrónicos?. Al respecto, el pronunciamiento fue el siguiente: “se debe señalar que frente al cumplimiento del régimen de protección de datos personales esta delegatura ha impuesto, desde la promulgación de la Ley 1581 de 2012 y hasta la fecha un total de 824 órdenes y 195 sanciones, las cuales repercuten en eficacia al mecanismo legal establecido por dicha norma.” (Carlos Salazar, 2021, Comunicación personal, Superintendencia de Industria y Comercio).

Conforme a los resultados de la investigación, el periodo de vigencia de la ley estatutaria y la respuesta de la Sic, se concluye que sí ha sido eficaz como garantía constitucional, sus mecanismos han demostrado con múltiples decisiones y manifestaciones que se aplican con la finalidad de proteger el derecho a la intimidad.

Referente al primer objetivo específico, identificar a través de los mecanismos legales de protección en la ley 1581 de 2012, las sanciones aplicadas por la Superintendencia industria y Comercio, a terceros por el mal manejo del habeas data. La presente investigación encontró que en efecto como se apreció en esta, existen bastantes sanciones

a entidades mayoritariamente privadas impuestas bajo los criterios legales y variando desde las económicas u órdenes para que cese el perjuicio por parte del tercero o terceros implicados.

Por último, frente al segundo objetivo específico, definir los mecanismos de protección existentes en la Ley 1581 de 2012, para ofrecer límites a los terceros que están encargados del tratamiento de datos personales. Se logra conseguir bajo el análisis y desarrollo concreto planteado en el segundo capítulo de la presente investigación.

En suma, hay aplicación de los mecanismos y funcionalidad del encargado de proteger los derechos inmersos en la ley estatutaria, en este caso la Sic como organismo administrativo ejerciendo sus labores, sin embargo, falta un compromiso de cumplimiento no solo de las empresas privadas que manejan datos personales sino también de la ciudadanía que permite precisamente sean estas las que los manejen arbitrariamente. Esto solo se puede lograr demostrando mayor interés, información, conciencia y empoderamiento de sus derechos.

Referencias

Aguilar Castañeda (2018). La ley de protección de datos en Colombia: sus inicios y examen de sus principales postulados, <https://repository.ucatolica.edu.co>.

Cifuentes, E. (1997). El Hábeas Data en Colombia. Derecho. Derecho PUCP: Revista de la Facultad de Derecho, ISSN 0251-3420, ISSN-e 2305-2546, N°. 51, 1997, págs. 115-144

Carlos Enrique Salazar Muñoz (2021). Comunicación personal vía derecho de petición. Superintendencia de industria y comercio. Radicación:21-102671-3

Corte Constitucional, sala plena (18 de agosto del 2010) Sentencia C-640. [MP Mauricio González Cuervo] www.corteconstitucional.gov.co

Corte Constitucional, sala plena (16 de octubre del 2008) Sentencia C-1011. [MP Jaime Córdova] www.corteconstitucional.gov.co

Corte Constitucional, sala plena (21 de junio del 2012) Sentencia SU 458. [MP Adriana María Guillen Arango] www.corteconstitucional.gov.co

Constitución política de Colombia, art. 15, 7 de Julio de 1991.

Constitución política de Colombia, art. 23, 7 de Julio de 1991.

Corte Constitucional, sala plena (17 de junio de 1992) Sentencia T-412 [MP Alejandro Martínez Caballero] www.corteconstitucional.gov.co

Corte Constitucional, sala plena (13 de junio de 1993) Sentencia T-340. [MP Carlos Gaviria Díaz] www.corteconstitucional.gov.co

Constitución política de Colombia, art. 44, 7 de Julio de 1991.

Corte Constitucional, sala plena (6 de octubre del 2011) Sentencia C-748. [MP Jorge Ignacio Pretelt Chaljub] www.corteconstitucional.gov.co

Corte Constitucional, sala plena (27 de enero del 2014) Sentencia T-020. [MP Luis Guillermo Guerrero Pérez] www.corteconstitucional.gov.co

Corte Constitucional, sala plena (23 de junio del 2005) Sentencia T-657. [MP Clara Inés Vargas Hernández] www.corteconstitucional.gov.co

Concepto n° 276941, Superintendencia de Industria y Comercio, 2013.

Corte Constitucional, sala plena (13 de febrero del 2018) Sentencia T-034. [MP Gloria Stella Ortiz Delgado] www.corteconstitucional.gov.co

Decreto 1377 de 2013(Presidencia de la república de Colombia) Art 2. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. 27 Junio de 2013. D.O 48834.

Decreto 1377 de 2013(Presidencia de la república de Colombia) Art 3. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. 27 Junio de 2013. D.O 48834.

Decreto 4886 de 2011, (Presidencia de la república de Colombia) Art 17.Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones. 23 Diciembre de 2011. D.O 48294.

Decreto 886 de 2014, (Presidencia de la república de Colombia) Art 5.Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. . 13 de Mayo de 2014. D.O 49150.

Dictamen del supervisor europeo de protección de datos sobre la comunicación de la comisión al parlamento europeo, al consejo, comité económico y social europeo y al comité de las regiones – un enfoque global de la protección de datos personales en la Unión Europea (2011, 14 de enero)

<https://edps.europa.eu/sites/edp/files/publication/11-01->

[14_personal_data_protection_es.pdf](https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_es.pdf).

Pérez, E. C., El procedimiento de habeas data: El derecho procesal ante las nuevas tecnologías,2017, Pg. 36.

Estudio de la Superintendencia de Industria y Comercio sobre medidas de seguridad en el tratamiento de datos personales hecho en noviembre 22 de 2019.

Buitrago, F. (2016), Aplicación de la ley estatutaria 1581 de 2012 en la red social Facebook. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, ISSN-e 1909-7786, N°. 15.

Faceta jurídica, Número. 76, Julio 2016, Pg61.

Garzón, García (J.R.) Protección de Datos Personales Ley 1581 de Octubre del 2012, 2015 pg 2. <http://www.unipiloto.edu.co>

González Guerrero, L. D. (2019), Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros.

Lanzarot, I. (2016). La protección jurídica de los derechos al honor a la intimidad personal y familiar y a la propia imagen de los menores. Actualidad jurídica iberoamericana, ISSN 2386-4567, N°. 5, 1, 2016, págs. 11-51.

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, D.O 4858, Art 2.

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, D.O 4858, Art 5.

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, D.O 4858, Art 7.

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, D.O 4858, Art 14.

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, D.O 4858, Art 15.

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, D.O 4858, Art 24.

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, D.O 4858, Art 25.

Ley 1437 de 2011, Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. D.O 47.956 Art 14.

Ley 1266 de 2008, Por la cual se dictan las disposiciones generales del habeas 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. D.O 47.219 Preámbulo.

Leyer, Faceta jurídica numero 65 septiembre y octubre de 2014''.

Ley 755 de 2015 art 32, Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo. D.O 49.559

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, D.O 4858, Art 23, Parágrafo.

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, D.O 4858, Art 16.

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. D.O 47.219 . Art 16 II N.6.

Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, D.O 4858, Art 22.

Bejarano, M. R. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales.

Remolina Angarita, N. (2010) ¿Tiene Colombia un nivel adecuado de protección de datos personales?.

Observación General No. 16, Comentarios generales adoptados por el Comité de los Derechos Humanos, Artículo 17 - Derecho a la intimidad, 32º período de sesiones, U.N. Doc. HRI/GEN/1/Rev.7 at 162 (1988).

Obando, V. J. (2020) Protección de datos personales en internet y su regulación el ordenamiento jurídico colombiano.

Cano, J; Remolina, Nelson; Rueda, Andrea; Pimentel, Javier; Ramírez, Ángela; Segrera, Martha E.; Iregui, Luis Andrés (2012). El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas.

Resolución Número 53593, 2020, Superintendencia de Industria y Comercio.

Rodríguez & Jaller, 2014, El habeas data como derecho fundamental y la ley 1581 del 2012 y su decreto 1377 del 2013, p. 86).

RAE-<https://dle.rae.es/telemetr%C3%Ada>.

Superintendencia de industria y comercio,2020, Guía sobre el tratamiento de datos personales en fotos, Pg 8.

Superintendencia de industria y comercio,2020, Guía sobre el tratamiento de datos personales en fotos, Pg 9.

Superintendencia de industria y comercio,2020, resolución número 62132, Hoja 25.

Superintendencia de industria y comercio, 2020, resolución numero 62132, Hoja 7.

Superintendencia de industria y comercio,2020, resolución número 62132, Hoja 28.

Superintendencia de industria y comercio, resolución 83882 de 2018, Hoja 11.

Superintendencia de industria y comercio, resolución número 44019,2020, pg 10.

Superintendencia de industria y comercio, Tramites y servicios,2020,

<https://www.sic.gov.co>,