PROTECCIÓN DE DATOS EN COLOMBIA. ANALISIS DE LA LEGISLACIÓN EXISTENTE

José Manuel Cipagauta Díaz

Licenciado en educación de la U.P.T.C

Abogado de la Universidad de Boyacá

Cipaman1000@gmail.com

Introducción

El concepto por el cual nace o inicia la protección de datos en el mundo, acontece a finales del siglo XIX, este se sintetiza en un artículo publicado en norte América, debido a la molestia que causaba la intromisión en la vida privada de los individuos, en este caso particular, un prestigioso abogado y su esposa, quienes tenían una vida social agitada y salpicada por escándalos, sin embargo, en aquella época dicha intrusión no era normal y desencadeno en la creación de lo que hoy conocemos como protección de datos.

Actualmente sobre todo en Europa y norte América, pero con avances en el resto del mundo, existen legislaciones muy completas respecto a este tema, que en el momento se encuentra más vigente que nunca, incluso llevando a algunos países a crear tribunales especiales y organismos expertos en estos temas, para garantizar dicha protección.

Es relevante aclarar que esta protección de datos, no se refiere a individualizaciones de entidades con datos gubernamentales, sino a datos personales, de cada individuo, que hacen parte de un fuero personalísimo y

que en un mundo cada vez más accesible y por así decirlo pequeño, debido a la globalización, deben ser amparados para evitar atropellos, que gracias al avance tecnológico pueden suceder en cualquier parte del globo.

Ahora bien, la finalidad particular de este artículo no es interferir en temas políticos o demostrar la competencia o incapacidad de nuestro legislador, más bien busca determinar tras una minuciosa revisión de las leyes sobre protección de datos personales, si dicha reglamentación es adecuada, suficiente y acorde para suplir las necesidades en la materia en un país como Colombia o por el contrario debe ser fortalecida o en el peor de los casos cambiar de rumbo.

Para esto se analizará cuidadosamente, pero a la vez de manera rápida, cada una de las leyes y decretos que regulan el tema de protección de datos en nuestro país, para finalmente encontrar unas conclusiones que, si bien serán de carácter personal, también estarán elaboradas de la manera más imparcial como nos sea posible.

Finalmente, dichas conclusiones apuntaran en dirección a afirmar que la legislación actual es suficiente o no lo es y en dado caso, de no serlo, cómo podría mejorar, siempre en busca de que sea una crítica constructiva y no un mero compendio de leyes y palabras sin un fin particular o sin un aporte practico a la sociedad.

Resumen

La protección de datos personales ha Cobrado gran relevancia a otros temas y jurisdicciones dentro de las legislaciones mundiales, en especial en los países con mayor desarrollo, como Norteamérica y la Unión europea, esto se debe en gran medida al avance tecnológico, hoy en día todos tenemos la mayor parte del tiempo una cámara y grabadora la mano, además ahora normalmente encontramos una en cada esquina de la calle, en los hogares y locales comerciales, asimismo todas las empresas guardan bases de datos con respecto a sus clientes y proveedores, también las redes sociales guardan datos, grabaciones e imágenes de sus usuarios, con muy poco control en la mayoría de los casos, este proyecto revisa de la manera más objetiva como sea posible la legislación colombiana en la materia de protección de datos, en busca de determinar si existe una legislación fuerte y con recursos, o sencillamente no, para esto se revisaron los antecedentes del tema a nivel mundial, ahondando en la reglamentación Colombiana, revisando y analizando el artículo 15 de la Constitución política, las leyes estatutarias 1266 de 2008 y 1581 de 2012, finalizando con el decreto 1377 de 2013 y comparándolos brevemente con legislaciones con mayores avances y mejores herramientas, en busca de conclusiones que esperamos compartan.

Abstract

The protection of personal data is becoming very important in world legislation, especially North American and European legislation, this is largely due to technological progress, today we all have a camera and recorder at hand, and now we usually find one in every street corner, in homes and

business premises, likewise all companies keep databases regarding their customers and suppliers, social networks also take data, recordings and images of their users, with very little control in most In all cases, this project reviews Colombian legislation on data protection in the most objective way possible, seeking to determine if there is strong legislation with resources, or simply not. For this, the background of the topic was reviewed. world level, delving into Colombian regulations, reviewing and analyzing article 15 of the Political Constitution, statutory laws 1266 of 2008 and 1581 of 2012, to end with the regulatory decree 1377 of 2013 and briefly comparing them with legislations with greater advances and better tools to reach conclusions that we hope you share.

Palabras clave

Dato personal, Base de datos, Titular, Tratamiento, Encargado del tratamiento, Responsable del tratamiento, Datos sensibles

Keywords

Personal data, Database, Owner, Treatment, Responsible for the treatment, Responsible for the treatment, Sensitive data

Capítulo I

"Privacidad" nacimiento de la protección de datos:

Para iniciar esta síntesis, es necesario tratar de manera sucinta y rápida los antecedentes legales a la protección de datos en el mundo y puntualizando en Colombia, por lo que se abordaran temas históricos, para finalizar examinando la legislación de nuestro país.

Todo esto con la finalidad de entender el por qué se hace necesaria la regulación en esta materia, sus inicios, cómo ha evolucionado y en qué estado lo encontramos actualmente, dándole prioridad al estado real del tema en nuestro querido país.

"La prensa sobrepasa en todas direcciones los límites obvios del decoro y la decencia. El chisme ya no es el recurso de los ociosos y los viciosos, sino que se ha convertido en un oficio que se persigue con industria y con descaro. Para satisfacer un gusto lascivo, los detalles de las relaciones sexuales se difunden en las columnas de los diarios. Para ocupar a los indolentes, columna tras columna se llena de chismes ociosos, que sólo pueden conseguirse mediante la intrusión en el círculo doméstico." **Warren, Samuel ; Brandeis, Louis (15 de diciembre de 1890). "El derecho a la privacidad" . Revista de derecho de Harvard.**

El anterior texto hace parte de lo que podemos entender como la primera intención escrita, de poner en la palestra publica la necesidad de regular la materia de la protección de datos personales, acuñada para una revista de la prestigiosa universidad de Harvard en 1890, se atribuye a Louis Brandeis como

a Samuel Warren, esté se basaría mayoritariamente en su "aborrecimiento profundamente arraigado de las invasiones de la privacidad social" como lo describen.

Ambos licenciados en derecho, expertos en leyes, discutieron como se podría proteger los derechos a la intimidad y buen nombre, lo lograron concatenándolos con el derecho a la personalidad y a la vez este con la vida y la propiedad, para formar así un concepto de derecho amplio, muy usado en el ordenamiento de los estados unidos, logrando influenciar a los legisladores norteamericanos para crear un concepto legal de privacidad, sin embargo, a este se llegó en principio gracias al derecho consuetudinario.

Así lo registro **Cazurro Barahona, V. (2020). Antecedentes y fundamentos del Derecho a la protección de datos**: "*Para ser más precisos, el nacimiento del concepto de privacidad suele situarse en la publicación del artículo "Right to Privacy", 1890, en el que los juristas investigaron las respuestas que ofrecía el entonces Vigente, derecho estadounidense ante las intromisiones en la vida privada de los individuos por parte de la prensa escrita."*

Poco más de 130 años han transcurrido, y ya se tenía claro que ningún derecho puede ser absoluto, todos tienen limitantes, como el que indica donde inicia el derecho de los demás, además de otros restrictivos dependiendo de la calidad del derecho, la protección de datos no es la excepción por lo que en su momento plantearon las siguientes limitantes al derecho a la "privacidad o intimidad":

“Sin embargo, ya entonces Warren y Brandeis señalaron que, aun siendo merecedor de protección, el ríght lo privacy o intimidad no era un derecho ilimitado (al igual que hoy, que en absoluto lo es). Para sostener esta afirmación elaboraron un cuerpo doctrinal sobre las limitaciones al derecho a la intimidad que, en su corpus central, ha llegado intacto hasta nuestros días. Según ellos, la noción de intimidad:

No impide la publicación de aquello que posea un interés público o general; y en este caso, es relevante la condición pública o privada del sujeto sobre el que verse la noticia, aunque hasta las personas públicas tengan el derecho a ver protegida una parte de su vida privada.

No excluye la publicación de determinados asuntos sobre hechos o manifestaciones relativos a instituciones o corporaciones públicas. ' Obliga a prestar atención a la conducta del afectado: así, consideran que el derecho a la intimidad decae con la publicación de los hechos por él mismo o con su consentimiento.

La intimidad ha de verse afectada de distinto modo en función del medio utilizado y el grado de publicidad de su vulneración; en este caso, el derecho no otorgaba reparación alguna por violación de la intimidad cuando la publicación de hechos se hiciera de forma oral y sin causar daños relevantes.”

Rebollo Delgado, (2008). Introducción a la protección de datos Madrid, España.

En Norteamérica se regularía este tema en su gran mayoría gracias a la jurisprudencia y el derecho consuetudinario, por lo que un país europeo tendría

el honor de crear la primera ley escrita de manejo y protección de datos, esto ocurrió en 1969, como lo muestra Oró Badia, en su libro, La protección de datos:

"Así, en 1969, el Gobierno del land alemán de Hesse hizo una amplia campaña propagandística sobre los beneficios que reportaría a los ciudadanos la existencia de un banco de datos centralizado con datos sobre salud, que incluyera la medicación habitual y las posibles alergias. De este modo, en caso de un accidente de tráfico, por ejemplo, la atención sanitaria que se podría prestar al accidentado sería mucho más eficiente: mediante la conexión a la base de datos se obtendría la información sanitaria relevante, lo que haría aumentar muy significativamente las posibilidades de sobrevivir. Pero en el mes de junio de aquel mismo año, se publicó un artículo en la prensa que advertía sobre los peligros que la informática representaba para los derechos de los ciudadanos, por lo que consideraba que había que hacer una ley sobre ellos. El tema impactó de tal manera en la opinión pública que el ministro presidente del land nombró una comisión para hacerla. Contrariamente a lo que suele suceder, la comisión acabó el trabajo, y el 7 de octubre de 1970 Hesse ya tenía aprobada su ley reguladora de bases de datos de la Administración. Nace así la primera ley de protección de datos personales del mundo."

Oró Badia, R. (2015). La protección de datos. Barcelona, España: Editorial UOC

Dicha ley procuraba brindar protección a personas naturales, excluyendo las jurídicas, resguardando así a cualquier persona ante la amenaza del tratamiento informático de los datos nominados por las autoridades y

administradores del Estado, municipios y demás entidades, así como el tratamiento dado por personas jurídicas de derecho público.

Con el ánimo de certificar el cumplimiento de los preceptos de dicha ley, esta creaba el cargo de, **Comisario de Protección de Datos** y uno de los más grandes aciertos, ya que garantizaba independencia para el desempeño de sus funciones.

Es claro que la legislación alemana es una de las más responsables en cuanto adelantos legales para la protección de sus ciudadanos, ante amenazas provenientes de su propio estado, por lo que imitando su cordura y ante el surgimiento de esta nueva necesidad, el concejo europeo a inicios de los años 70, preocupado por la intromisión en los datos personales, debido a la aparición de la informática y todo lo que consigo acarrearía, se propone promulgar un acuerdo con fuerza de ley, para lo que designa un concejo especial, que tardo más de 10 años en este propósito.

Hasta que finalmente en 1981 se firma el convenio 108, que define por primera vez, datos personales, privacidad y otros conceptos muy amplios que no se habían tratado anteriormente, pero de vital importancia en el derecho moderno, así lo documento **Cazurro Barahona, (2020). Antecedentes y fundamentos del Derecho a la protección de datos. Barcelona, España**:

“Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal

(«Convenio 108»)

Capítulo I. Disposiciones generales

El fin del presente convenio es garantizar, en el territorio de cada parte, a cualquier persona física, sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de datos de los datos de carácter personal correspondientes a dicha persona (protección de datos).”

Así nace una jurisdicción europea de protección de datos y privacidad de las personas, el cual regulo de manera obligatoria el tema en Europa, aunque actualmente y con nuevos avances han logrado que se acojan incluso países tan lejanos como Uruguay.

En Colombia el primer preocupado por el tema de protección de datos, fue la Corte constitucional en el año de 1991, plasmándolo en el artículo 15 de la norma de normas, el cual se encuentra en el Capítulo 1 “de los derechos fundamentales” pero que tiene muy poco desarrollo, ya que realiza un repaso muy sucinto de lo que comprende y lo que debe proteger y garantizar el estado respecto a la intimidad personal, el buen nombre y habla de bases de datos.

Pero no fue sino hasta el año 2008 que se dio el primer paso en materia legal de protección de datos, pero solo preocupados por habeas data y protección de lo contenido en bases de datos.

Al fin en el año 2012 se tomó en serio el tema y se dictó la ley general que regula la materia de protección de datos personales, definiendo en la misma ley que a más tardar en un año se reglamentaria a través de decreto dicha norma.

Y así fue como apareció el decreto 1377 de 2013.

Capitulo II

Treinta años de legislación en 10 páginas:

En Colombia la normatividad en protección de datos personales aparece a finales del siglo pasado con la constitución de 1991 así:

*"**ARTICULO 15. Constitución Política**: 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"

De este artículo se desprende la legislación actual colombiana en manejo y protección de datos, que tienen carácter de sensibles y se elevan al nivel de derechos fundamentales, es un gran inicio, aunque el posterior desarrollo normativo fue precario y no duplico los aciertos de otras legislaciones.

En su momento trato temas que no se habían dilucidado anteriormente, como la inviolabilidad de la información personal, tema no regulado y que por

consiguiente daba gran poder a los administradores de bancos de datos, guardianes o administradores de correspondencia y datos personales.

Constitución Política de Colombia. Art. 15. Julio 20 de 1991.

El espíritu del artículo constitucional, es tener en cuenta temas invisibles hasta el momento, como las nuevas tecnologías y casi que profetiza lo que se viene, respecto al tema informático a las cámaras de vigilancia, hoy con varias en cada esquina, negocio o residencia y que toman de las personas lo más íntimo, su ser, su rostro, su aspecto, sus secretos y muchas más cosas que anteriormente no alcanzábamos ni a imaginarnos, así como la estampida de las redes sociales en la sociedad actual.

ley 1266 de 2008:

No fue sino hasta casi 20 años después que Colombia por fin expidió una ley que regulara el tema de la protección de datos, sin embargo, esta se enfoca principalmente en el amparo al Habeas data y la información contenida en bases de datos, en especial la información financiera, crediticia, comercial y de servicios, por lo tanto, se trataran los temas más relevantes de la ley.

Además, con el ánimo de no convertir este artículo en una transcripción larga y aburrida, el artículo se alejará del literal de la ley, para acercarnos un poco más a su espíritu, buscando realizar un análisis rápido del texto, pasando por alto apartados que sean considerados de poca incidencia en la norma, como los que solo son requisitos de forma legal.

De esta manera el lector tendrá a medida que avanza, la facilidad de sacar rápidas conclusiones de las normas analizadas, aunque siempre se puede remitir a estas y revisar su tenor, para realizar un análisis más profundo.

Artículo 2°. Esta ley se aplicará a los datos de información personal registrados en bases o bancos de datos, excepto los que ayudan a la Inteligencia de Estado por parte del, DAS, y de la policía, para garantizar la seguridad nacional y se excluyen también de la ley aquellos datos mantenidos en un ámbito exclusivamente doméstico e íntimo”

Artículo 4°. Principios de la administración de datos. **Principio de veracidad**. La información debe ser veraz y completa, se prohíben datos que induzcan a error. **Principio de finalidad.** La administración de datos debe apegarse a la Constitución y la ley. **Principio de circulación restringida**. Debe limitarse según naturaleza de los datos. **Principio de temporalidad de la información**. La información no podrá ser suministrada cuando deje de servir para su finalidad. **Principio de interpretación integral de derechos constitucionales**. Se interpretará acorde y armónicamente con los derechos constitucionales aplicables. **Principio de seguridad.** La información se manejará con las medidas para garantizar la seguridad de los registros. **Principio de confidencialidad.** Los que intervengan en la administración de datos que no sean públicos, están obligadas a garantizar reserva de la información.

artículo 5°. circulación de información. La información recolectada por los operadores de la base o banco de datos, podrá ser entregada o puesta a disposición de las siguientes personas a) A los titulares, o las personas

debidamente autorizadas por estos b) A los usuarios de la información. c) A cualquier autoridad judicial, previa orden judicial. d) A las entidades del poder ejecutivo, cuando dicha información corresponda directamente al cumplimiento de alguna de sus funciones. e) Órganos de control y dependencias disciplinarias, fiscales, o administrativa, cuando la información sea necesaria para el desarrollo de una investigación f) Otros operadores de datos, cuando se cuente con autorización del titular. g) Otras personas autorizadas por la ley.

Artículo 6°. derechos de los titulares de la información.

1. Frente a los operadores de los bancos de datos: (i) Ejercer mediante los procedimientos de consultas o reclamos el derecho fundamental al hábeas data en los términos de la presente ley. (ii) Solicitar el respeto y la protección de los demás derechos constitucionales o legales. (iii) Solicitar prueba de la autorización expedida por la fuente o el usuario. (iiii) Solicitar información acerca de los usuarios autorizados para obtener información.

2. Frente a las fuentes de información: (i) Ejercer su derecho fundamental al hábeas data y petición, sin perjuicio de más mecanismos. (ii) Pedir información, actualización o rectificación, lo realizará el operador, con base en la información aportada (iii) Solicitar prueba de la autorización, cuando sea requerida conforme a la presente ley.

3. Frente a los usuarios (i) Inspeccionar la utilización que el usuario le está dando a la información, cuando la información no fue suministrada por el operador. (iii) Solicitar prueba de la autorización, cuando ella sea requerida.

Artículo 7°. deberes de los operadores de los bancos de datos.

A). Garantizar, el hábeas data y petición, así como dar a conocer la información que del titular exista, y solicitar la actualización o corrección. B) En la recolección y tratamiento se respetarán los demás derechos. C) Permitir acceso a la información a las personas que, según la ley, pueden tener acceso a ella. D) Asegurar el adecuado cumplimiento de la presente ley. E) Solicitar a la fuente la autorización otorgada por el titular. F) Conservar los registros almacenados para impedir su deterioro, pérdida, alteración. G) Realizar periódica y oportunamente actualización de datos, H) Tramitar las peticiones, consultas y los reclamos formulados por los titulares. I) Indicar en el registro que la información se encuentra en discusión, cuando se haya presentado solicitud de rectificación o actualización y no haya finalizado dicho trámite. J) Circular la información a los usuarios. K) Cumplir las instrucciones que las autoridades impartan L) Los demás que deriven de la Constitución o de la presente ley.

Como se puede establecer en el estudio de la presente ley, se enfoca exclusivamente en los procedimientos para tramitar habeas data y peticiones de informaciones contenidas en bases de datos.

Impone un sistema completo, hay que reconocerlo, para la recolección, modificación, rectificación, traspaso y todo lo referente a la información personal contenida en bases de datos, y como se supone, que es el titular de dicha información quien de primera mano, pueda acceder a está, sin embargo, no regula ningún tema referente a la intimidad o fuero personal, tampoco a temas de datos sensibles recolectados por medios tecnológicos como cámaras,

grabaciones y otros, tampoco el tema de las ya existentes redes sociales o telefónicas y muchos más.

Así no lo hizo saber también la corte constitucional en sentencia C-748 DE 2011: "*En el caso colombiano, el proyecto de ley que dio lugar a la Ley 1266 de 2008 y que fuera objeto de la sentencia C-1011 de 2008, buscaba convertirse en una ley de principios generales aplicable a todas las categorías de datos personales, pero pese a su pretensión de generalidad, el proyecto de ley en realidad solamente establecía estándares básicos de protección para el dato financiero y comercial destinado a calcular el nivel de riesgo crediticio de las personas. Por ello en la referida sentencia, la Corte dejó claro que la materia de lo que luego se convertiría en la Ley 1266 es solamente el dato financiero y comercial. Por lo tanto, la Ley 1266 solamente puede ser considerada una regulación sectorial del habeas data. Ahora, con el nuevo proyecto de ley se buscará llenar el vacío de estándares mínimos de protección de todos los datos personales, de ahí que su título"*

Ley 1581 de 2012:

Así en el 2012 se promulga la ley estatutaria 1581 de 2012 "**Por la cual se dictan disposiciones generales para la protección de datos personales**" a la cual también, se le debe realizar una revisión completa.

Artículo 4°. Principios para el Tratamiento de datos personales. a) **Principio de legalidad:** El Tratamiento a que se refiere la presente ley es una actividad reglada; b) **Principio de finalidad:** Se debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley;

c) **Principio de libertad:** Sólo se pueden tratar los datos con el consentimiento del Titular, o con mandato legal o judicial; d) **Principio de veracidad:** La información debe ser veraz y completa, se prohíben datos que induzcan a error e) **Principio de transparencia:** Se debe garantizar al Titular el obtener información acerca de la existencia de datos que le conciernan; f) **Principio de acceso y circulación restringida:** Debe limitarse según naturaleza de los datos**,** sólo podrá hacerse por personas autorizadas. Los datos, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva; g) **Principio de seguridad:** El Responsable del Tratamiento, se deberá manejar con las medidas necesarias para otorgar seguridad a los registros; h) **Principio de confidencialidad:** Los que intervengan en la administración de datos que no sean públicos, están obligadas a garantizar reserva de la información.

Artículo 5°. Datos sensibles. Son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Artículos 6 y 7: Se prohíbe de cualquier manera el tratamiento de los datos anteriormente nombrados, con algunas excepciones lógicas, como por orden judicial, o por intereses nacionales y otros.

Además, los niños niñas y adolescentes tienen derechos prevalentes, la presente ley no es la excepción, por lo que es necesario capacitar a las

distintas entidades para tener en cuenta el uso debido y responsable de los datos de los menores.

Artículo 9°. Autorización del Titular. El Tratamiento requiere la autorización previa del Titular y debe obtenerse por un medio que pueda ser consultado posteriormente.

El articulo 10 contempla las excepciones en las cuales no será necesaria la autorización del titular, son lógicas: por urgencia médica, datos públicos, orden judicial.

Artículo 11. Suministro de la información. Podrá ser suministrada por cualquier medio, según lo requiera el titular. Deberá ser de fácil lectura, sin barreras técnicas y deberá corresponder a aquella que repose en la base de datos.

Artículo 12. Deber de informar al Titular. El responsable del tratamiento de los datos deberá informar al titular a) El Tratamiento al cual serán sometidos sus datos y la finalidad; b) El carácter facultativo, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes; c) Los derechos del Titular; d) La identificación, dirección y teléfono del responsable del Tratamiento.

Respecto a los artículos 9 al 12, debemos decir que: las posibilidades son tantas y tan amplias que es casi imposible que las personas se enteren o siquiera se percaten de que están dando uso a sus datos, de la forma que sea, esto es, con apego a la ley o infringiendo todas o algunas las reglas establecidas en la presente norma.

Mas aún, en muchos de los casos quienes tratan los datos o quienes los administran, no son personas idóneas, para estos fines, personas sin ninguna capacitación y posiblemente con desconocimiento de la ley, por lo que disponen de hecho de estos datos, violando un derecho fundamental de los titulares de estos datos.

Tenemos como ejemplo, el encargado de la vigilancia que debe subir a una nube digital o disco duro las grabaciones de las cámaras de seguridad, para reiniciar las cintas o sencillamente para que no se exceda la capacidad, tiene la potestad de definir que archiva y que borra, con unos parámetros que en nada se parecen a los dados por el contenido normativo, más bien lo hace con las directrices dictadas por la necesidad o en el mejor de los casos por la empresa para la que labora, pautas que seguramente no guardan apego a la regla legal existente. Finalmente, el dirigente del conjunto termina administrando dichos datos guardados, nuevamente sin conocimiento legal alguno.

Como vemos la norma regula un porcentaje pequeño de los datos personales que encontramos hoy en día, teniendo presente que la mayoría de las bases de datos y datos dispersos se encuentran en manos de personas que no saben que los poseen, por lo que aplicación de la leyes limitada y frívola, ya que la protección de los derechos no se realiza de oficio, ni se incoa el amparo de estos.

Artículo 14. *Consultas*. El titular podrá consultar su información en cualquier base de datos, el responsable del tratamiento deberá suministrar la información, se formulará por el medio habilitado, siempre que se pueda tener prueba de esta.

La consulta será atendida máximo en (10) días hábiles. Cuando no fuere posible, se informará al interesado los motivos de la demora y señalando la fecha, la cual no podrá superar los cinco (5) días hábiles tras el vencimiento del primer término.

Artículo 15. Reclamos. Quien considere que su información debe ser corregida o actualizada, podrá reclamar ante quien administra sus datos, con estas reglas.

1. Con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si resulta incompleto, se requerirá al interesado dentro de (5) días para que subsane las fallas. Tras dos (2) meses del requerimiento, sin que se presente la información, se desiste del reclamo. 2. Recibido el reclamo, se incluirá leyenda "reclamo en trámite" y el motivo, en un término no mayor a dos (2) días y deberá mantenerse hasta que sea decidido. 3. El término para resolver será de (15) días. Si no es posible atenderlo, se informarán los motivos de la demora y se resolverá en los ocho (8) días siguientes. EL RECLAMO ANTE LA SIC, tiene como requisito de procedibilidad haber agotado consulta o reclamo ante quien administra sus datos.

Artículo 17. Deberes de los responsables del Tratamiento. a) Garantizar, en todo tiempo, el derecho de hábeas data; b) Conservar, copia de la respectiva autorización otorgada por el Titular; c) Informar al Titular la finalidad de la recolección y los derechos que le asisten; d) Conservar la información bajo seguridad que impida su adulteración o pérdida y acceso no autorizado o fraudulento; e) La información que se suministre sea veraz, completa, exacta y

actualizada; f) Actualizar la información y mantenerla así, comunicando todas las novedades respecto de los datos; g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado; h) Suministrar al Encargado, únicamente datos previamente autorizados; i) Exigir al Encargado, el respeto de la seguridad y privacidad de la información del Titular; j) Tramitar consultas y reclamos en los términos señalados; k) Adoptar manual de políticas y procedimientos para la atención de consultas y reclamos; l) Informar al encargado cuando la información se encuentra en discusión por parte del Titular, por reclamación que no haya finalizado; m) Informar a solicitud del Titular sobre el uso dado a sus datos; n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad o existan riesgos. o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

En relación a deberes, consultas reclamos o modificaciones del contenido en bases de datos, se plantea nuevamente el inconveniente y que tal si

a- desconozco la existencia de dicha referencia o base de datos, en la cual estoy relacionado.
b- Quienes poseen o administran el banco de datos, ignoran la existencia de dicha información ya sea que se administra de manera automática o debido al descuido en el manejo de esta.
c- Los dos anteriores escenarios convergen.

Las inquietudes que nos generan los anteriores escenarios son desalentadoras: (i) quien me garantiza la protección de datos que nadie sabe que existen; (ii) quien solicita o incoa la protección de dichos datos (i) que

autoridad vigila o conoce estos casos, en el entendido que más que un juzgador, se debe tratar de una unidad investigativa.

Los deberes del encargado del tratamiento de los datos son similares y además lógicas también, posteriormente la ley habla de un tema muy importante: **la autoridad de protección de datos**.

Para lo cual se designa a la Super Intendencia de Industria y Comercio (SIC) a través de una delegación para ejercer las funciones de Autoridad de Protección de Datos, que es creada por esta ley y que debía fundarse a más tardar seis meses después de la promulgación de la ley.

No establece un procedimiento, más bien genéricamente se refiere a que impondrá las sanciones respectivas y dicta que lo no reglado en esta ley se surtirá bajo el procedimiento del código Contencioso Administrativo.

Impone a la SIC unas funciones bastante genéricas y lógicas siendo hasta el momento y según esta ley, la única autoridad en la protección de datos, que por ahora existe en el país.

Entre sus funciones destacan la de ser el único administrador del registro Nacional público de bases de datos, que es como su nombre lo indica el directorio de bases de datos en Colombia, que es de libre consulta por cualquier ciudadano, También la (SIC) debe emitir las órdenes y los actos administrativos que regirán esta entidad.

Además, y muy importante, es el enlace con entidades extranjeras o internacionales cuando la actuación de estas afecte a un titular de datos que sea ciudadano colombiano.

Finalmente contempla unas sanciones que se aplicaran solamente a personas de naturaleza privada, así: (i) hasta 2000 smlmv. (ii) suspensión de actividades hasta por 6 meses y adopción de correctivos. (iii) cierre temporal, si no aplica los correctivos. (iv) cierre definitivo.

Además, contempla los criterios para graduación de estas sanciones, que son: a) Según el beneficio económico obtenido b) dependiendo del daño causado.

Esta ley claramente regula temas de interés y protección de datos con una mayor profundidad, pensando en la intimidad personal, el fuero interno, las grabaciones y otros, además crea el órgano que debe estar al pendiente de ello.

sin embargo, sin tocar algunos temas importantes, como la persecución a infractores, órganos de naturaleza judicial y correctivos más fuertes, para no decir que reales, ya que siendo normalmente empresas (personas jurídicas) las que recolectan y administran los datos, estas simplemente cierran e inician, o usan presta nombres, practica muy común en nuestro país, así que se evadirán las multas, el cierre no será una sanción real, en cambio sí se puede causar mucho daño sin la real protección de los datos personales y otros tipos de datos sensibles, como su filiación política, su origen racial y las que puedan afectar su vida íntima.

Estas falencias en la regulación respecto al manejo que se da a la protección de datos, dando lugar a la intromisión en la intimidad de las personas y otros derechos, la demostró también la corte constitucional:

T-643 de 2013: “¿Vulnera una persona los derechos a la propia imagen, la intimidad, el buen nombre y la honra de otra, cuando se niega a retirar las imágenes de esta última de un sitio web abierto al público y de otros medios de publicidad sobre los que tiene control, cuando (i) las imágenes fueron tomadas y divulgadas con base en una autorización general para ser usadas con fines publicitarios no específicos; (ii) quien aparece en ellas nunca consintió expresamente en que fueran divulgadas en un contexto en el cual aparece proyectada en un rol que puede ser asociado a la prestación de servicios sexuales; y (iii) esto ha tenido efectos negativos en su vida familiar y social?”

La respuesta dada en la anterior sentencia, fue **SI** se vulneran los derechos a la intimidad, a la imagen propia, al buen nombre y revocando las sentencias de instancias anteriores, amparo estos derechos.

Complementando la norma y mostrando que se encuentra imperfecta, respecto a algunos temas, como el tratado en esta sentencia de constitucionalidad y otros que hacen parte de los derechos personales.

DECRETO 1377 DE 2013:

Es el que reglamenta entre otras la ley 1581 de 2012, vista anteriormente y además ley general de protección de datos en Colombia.

Realmente no reglamenta mucho, simplemente realiza algunas aclaraciones que ya se encontraban en la ley 1266 de 2008, que no está derogada, realiza algunas adiciones a la ley 1581 y reglamenta lo que veremos a continuación, también nos da algunas definiciones que también se caracterizan por ser lógicas y estar en el diccionario.

Se esperaría mucho más del decreto reglamentario de una ley estatutaria general, algunos esperábamos un código, que es de vital importancia en la actualidad, por el tema que regula.

Artículo 4°. Recolección de los datos personales. Con los principios de finalidad y libertad, la recolección de datos se limitará a que son pertinentes y adecuados para su finalidad. Salvo los previstos en la ley, no se recolectarán datos sin autorización.

A solicitud de la SIC, los responsables deberán explicar los procedimientos usados para la recolección, almacenamiento y uso, como también de las finalidades para las cuales la información es recolectada y sobre la necesidad de recolectar los datos.

No se podrán usar medios falaces para recolectar y realizar Tratamiento de datos.

Artículo 23. Medios para el ejercicio de los derechos. Todo Responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos, que dará trámite a las solicitudes, para el ejercicio de los derechos del titular.

El decreto se refiere de manera genérica a varias leyes, para el desarrollo del presente artículo, solo nos interesa lo referente a la ley de protección de datos 1581 de 2012.

Podemos ver que, aunque se trate de un decreto reglamentario, la vez no lo hace, ya que realmente solo agrega algunos numerales a artículos ya existentes, es más un complemento normativo que una reglamentación.

Llama especialmente la atención artículos tan amplios y en blanco como el siguiente:

“*Limitaciones temporales al Tratamiento de los datos personales* *. Los responsables y Encargados del Tratamiento solo podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento”*

También dice que después de este tiempo, que no dice cuál es, se deben suprimir los datos, sin embargo, deben ser conservados, si así se requiere.

Como podemos ver, no existe entidad que regule, el tiempo por el cual se deben tratar los datos de las personas, ese término tratar es un término más cercano a comercializar, se suponía que el decreto lo haría, pero no, así encontramos otra cosa que queda en el aire, además es muy contradictorio en cuanto a si se debe o no destruir estas bases de gran valor comercial.

Afectaciones a la intimidad o privacidad:

“Bogotá. D.C., 02 de mayo de 2019. La Superintendencia de Industria y Comercio a través de la delegatura de datos personales ratificó la multa impuesta al EDIFICIO CARRERA SÉPTIMA PROPIEDAD HORIZONTAL por un valor de $78.124.200 por no cumplir las normas de recolección de datos personales. Luego de una visita de inspección realizado por la SIC al inmueble se encontraron varias irregularidades:

- *Recolectar sin autorización de las personas sus datos como lo son las imágenes de fotos y las grabaciones de videovigilancia.*

- *No contar con mecanismos para garantizar la seguridad y confidencialidad de la información.*
- *No tener una política de tratamiento de datos que se ajustara a las exigencias de la Ley 1581 de 2012 y sus normas reglamentarias.*
- *No informar a los visitantes del edificio sobre sus derechos, finalidades y demás exigencias del artículo 12 de la ley 1581 de 2012.*

La SIC recordó que los edificios de oficinas o conjuntos residenciales que se someten al régimen de propiedad horizontal son personas jurídicas responsables del tratamiento de los datos que recolectan, almacena o usan, sobre todas las personas que ingresan a sus instalaciones. Por lo tanto, están obligados a cumplir la Constitución y las leyes 1581 de 2012 o 1266 de 2008.

Además, las fotos e imágenes de videovigilancia son datos biométricos, catalogados como información sensible por el artículo 5 de la Ley 1581 de 2012. La información biométrica incluye datos sobre las características físicas (rostro, cuerpo, huella dactilar, palma de la mano, retina, ADN). Para tratar lícitamente este tipo de datos es necesario obtener una autorización previa, expresa, informada y especial." **Super intendencia de Industria y Comercio de Colombia. (2015) www.sic.gov.co.**

Del texto anterior se desprende una conclusión importante, casi todos los datos captados por una cámara tienen el carácter de sensible.

Y con especial protección de los datos biométricos que son personalísimos, que revelan, no solo la identidad de las personas, sino secretos fácilmente debelados por la pantalla sin necesidad de un profundo análisis.

Si bien en este punto la SIC se mostró preocupada por sentar un precedente, iniciando el proceso sancionatorio a infractores de la ley, el empellón duro poco y actualmente las cámaras de videovigilancia, no solo de los conjuntos cerrados, sino de los locales comerciales, empresas, hogares, prestadores de servicios públicos y entidades públicas se encuentran sin regulación y vigilancia y casi que en la anarquía total.

Si bien es cierto entre 2019 y 2020 se incrementó ante la SIC en un 27% el número de quejas presentadas por violación a la protección de datos y un 25% en 2021, según datos de la misma entidad, estas son en su gran mayoría, el 90%, por infracciones a la ley del habeas data financiero.

Dejando con un escaso 10% la protección de datos personales, es decir de las casi 20.000 quejas recibieron en 2021 solo 2.000 son por la indebida protección de datos personales y el 71% de estas es decir 1.420 son por falta de autorización para recolectar u usar los datos personales, dando a todos los demás delitos, afectaciones e infracciones posibles, solo 680 quejas en 2021.

Estos delitos, infracciones y afectaciones que se pueden ocasionar en el ámbito de la protección de datos actualmente van relacionados en su mayoría de la mano con la informática, que rige el 99% de la recolección actual de datos con contadas excepciones de archivos físicos que puedan aun existir.

Ahora veremos los principales delitos cometidos. Según un estudio de la universidad de Zulia, los principales delitos contra los datos personales en América latina son:

a) Acceso no autorizado: la única manera de lograr esto es a través de la violación de los datos personales.
b) El espionaje informático con fines de recolección de datos.
c) Robo de identidad.
d) La interceptación no autorizada
e) Manipulación de datos de ingreso.

Ahora bien, el mismo estudio nos dice que las principales causas de los delitos contra los datos personales en Latinoamérica se deben o están relacionados con:

1- Bancos de datos ilegales o irregulares.
2- Falta de información.
3- Redes sociales.
4- E- mails.
5- Nubes recolección de información.

En este punto del artículo, debemos a modo de ejercicio realizarnos las siguientes preguntas respecto a nuestra legislación ¿tenemos suficiente? ¿Debemos conformarnos con lo que tenemos? En caso de que creamos que hace falta algo, ¿Cómo podemos mejorar? Cada uno llegara a sus propias conclusiones, pero mientras tanto, veamos las mías.

Conclusiones

En este artículo se evidencia la escasa legislación actual en Colombia, la que además está llena de vacíos legales, la que rige de manera superflua un tema tan relevante jurídicamente hablando, como es la protección de datos personales, datos que tienen el carácter de sensibles y se elevan al nivel de derechos fundamentales según la constitución, norma de normas, pareciera que su regulación se debe más a una continuación despreocupada de lo que en algún momento plasmo el constituyente en el año 1991 y no un ejercicio consiente, preocupado por proteger los datos de las personas del común.

Se puede observar que se legisla de forma simple y sin ahondar, más bien parece se hizo por compromiso, no por un interés legítimo de regular un tema tan actual y tan importante, por la cantidad de posibilidades que dan las nuevas tecnologías, que debería convertir la protección de datos y lo que de esto deriva, en legislaciones muy extensas, con desarrollados códigos legales y regulaciones completas, como lo serán las legislaciones de los grandes países.

También, es notorio que, al ser la legislación muy básica, igualmente lo es la invocación al amparo de estos derechos, ya que, si el legislador conoce muy poco del tema, mucho menos comprenderá la ciudadanía que debe incoar a través de las jurisdicciones existentes la garantía de sus derechos.

Ahora, claramente si es escasa la oferta y la demanda, también lo será la jurisprudencia, no solo es poca, sino que se queda corta, se refiere y regula mayoritariamente temas de *habeas data*, y la protección de datos personales que se encuentran en bases de datos, además las podemos contar con la

mano, entre las pocas que existen y de las cuales se recomienda también una juiciosa lectura son:

t-414 de 1992. a) La dignidad humana, principio Constitucional supremo; b) La nueva tecnología y su relación con la libertad personal.; c) Intimidad y habeas data; d) Intimidad y el derecho a la información; e) Los Datos y sus propietarios; f) Bancos de datos y derecho informático; g) Usos responsables de la Informática.

Corte Constitucional colombiana, sala plena (Magistrado Ponente, Ciro Angarita Barón, **16 de junio de 1992) Sentencia No. T-414/92.**

Su-082 de 1995. a) La forma como cualquier persona cubra sus obligaciones económicas, pertenece a su intimidad personal; b) Habeas data, contenido y medios para su protección; c) Conflicto entre derecho a la información y buen nombre; d) Límite temporal de la información, caducidad de datos.

Corte Constitucional colombiana, sala plena (presidente, Jorge Arango Mejía, **1 de marzo de 1995) Sentencia No. SU-082/95.**

T-729 de 2002**.** a) Alcance del derecho al habeas data b) Principios fundamentales en la administración de datos personales.

Corte Constitucional colombiana, sala plena (Magistrado Ponente, Eduardo Montealegre Lynett, **5 de septiembre de 2002) Sentencia T-729/02.**

C-334 de 2010**.** a) Información genética b) Los datos personales que son de carácter público, privado, semiprivado y los reservados.

Corte Constitucional colombiana, sala plena (Magistrado ponente, Juan Carlos Henao Pérez, 12 de mayo de 2010) Sentencia C-334/10

SU 458 de 2012: Bases de datos que contienen los antecedentes penales, datos personales sobre antecedentes y sus Principios.

Corte Constitucional colombiana, sala plena (magistrada ponente, Adriana María Guillén Arango, 21 de junio de 2012). Sentencia SU458/12

T-987 de 2012. Registros de información desfavorable o llamadas "*listas negras*", como los principios del habeas data son límites al tratamiento de los datos personales.

Corte Constitucional colombiana, sala plena (magistrado ponente, Luis Ernesto Vargas Silva, 23 de noviembre de 2012). Sentencia T-987/12

Algunos países han designado autoridades espéciales para la protección de los datos o para vigilar a quienes recolectan, tratan, administran o hacen circular estos, no solo respecto a las bases de datos, sino los datos personales captados por cámaras de vigilancia o web.

Además, se han creado hasta tribunales especiales y se decretaron penas pecuniarias, pero llama mucho la atención, que existen penas de privación de la libertad, mostrando la relevancia con que se están tomando este tema y la seriedad que desean trasmitir a los destinatarios de estas leyes.

Se constituyen también órganos con absoluta independencia de las ramas del poder, evitando intromisiones de dichos poderes y asegurando la imparcialidad.

Es de notar que la legislación europea es muy protectora de los datos, prohíbe grabar indiscriminadamente y así proteger la intimidad de las personas, incluyendo cualquier transeúnte:

Gil Membrado, C. (2019). Videovigilancia y protección de datos. Madrid, España: *"Pronunciamiento de la Audiencia Nacional, en esta ocasión dado por Sentencia de 4 de noviembre de 2014, que parte de la instalación de cámaras de videovigilancia en sucursales del Banco Popular Español que captaban imágenes de personas que transitaban por la calle Velázquez de Madrid y por el paseo de Gracia de Barcelona sin su consentimiento.*

La Sala considera que la grabación de imágenes para ver «lo que ocurre en el exterior de la oficina bancaria cuando se encuentran bajadas las persianas blindadas instaladas para proteger la sucursal y sus empleados» rebasa los límites del legítimo derecho a proteger la seguridad de sus instalaciones y de su personal, ya que vulnera el derecho a la protección de datos de las personas que se encuentran transitando la vía pública."

Al parecer, lo que se ha regulado en tema de datos por la legislación colombiana va gradualmente un paso atrás respecto a lo que debería ser y que se puede ver en otros países. Esto se debe a que las leyes y decretos acá analizados muestran una urgente necesidad de complementos normativos, mayor reglamentación o la expedición de nuevas y más completas leyes.

Se puede concluir que la legislación colombiana si bien tiene algunos avances legales, complementados por la jurisprudencia, debe de manera

urgente reglamentar en muchos aspectos la protección de los datos personales.

Faltan muchos asuntos por regular, si lo comparamos con los avances que han tenido otros países y legislaciones, existe un progreso, claro, pero se debe entender que la tecnología florece a pasos gigantes y a la par deben ser protegidos los datos por esta recolectados.

Es urgente regular los temas de información captada por aparatos tecnológicos y redes, incluyendo redes sociales, así como los datos que en estos lugares se recolectan, los que salen a la luz y los que no, los que revelan temas de la personalidad o físicos, actualmente un poco olvidados.

Debemos tener en cuenta que la gran mayoría de los datos personales recogidos, incluyendo los de las redes sociales, se usan con fines comerciales.

Siendo un tema comercial y no jurídico, no podemos esperar escrúpulos y mucho menos legalidad por parte de quienes captan, administran y comercializan los datos**,** por lo que en mi concepto necesitamos una legislación mucho más robusta, férrea, con herramientas y que no tenga vacíos, si queremos enfrentar los retos que llegan con las nuevas tecnologías y la recolección de datos personales que estas realizan.

Conclusión final: la legislación colombiana debe ser FORTALECIDA.

REFERENCIAS

Gil Membrado, C. (2019). Videovigilancia y protección de datos. Madrid, Wolters Kluwer España. https://elibro.net/es/ereader/usta/111656?.

Cazurro Barahona, V. (2020). Antecedentes y fundamentos del Derecho a la protección de datos. Barcelona, J.M. BOSCH EDITOR. https://elibro.net/es/ereader/usta/130485?.

Warren, Samuel ; Brandeis, Louis (15 de diciembre de 1890). "El derecho a la privacidad" . Revista de derecho de Harvard. https://harvardilj.org/2021/05/taking-down-one-of-the-worlds-largest-and-more-profitable-criminal-industries-trafficking-in-persons-part-ii-libya-and-central-america/.

Rebollo Delgado, L. (2008). Introducción a la protección de datos (2a. ed.). Madrid, Spain: Dykinson. https://elibro.net/es/ereader/usta/63115?.

Oró Badia, R. (2015). La protección de datos. Barcelona, Spain: Editorial UOC. https://elibro.net/es/ereader/usta/57741?page.

Super intendencia de Industria y Comercio de Colombia. (2013). Cartilla formatos modelo para el cumplimiento de obligaciones establecidas en la ley 1581 de 2012 y sus decretos reglamentarios. www.sic.gov.co

Constitución Política de Colombia. Art. 15. Julio 20 de 1991. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica 1991html

Ley estatutaria 1266 de 2008 (diciembre 31-2008). 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, Diario Oficial No. 47.219 de 31 de diciembre de 2008 http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

ley estatutaria 1581 de 2012 (octubre 17-2012) Por la cual se dictan disposiciones generales para la protección de datos personales, Diario Oficial No. 48.587 de 18 de octubre de 2012 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Decreto 1377 de 2013 (junio 27-20013) por el cual se reglamenta parcialmente la ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646.

Página web de la Superintendencia de Industria y Comercio http://www.sic.gov.co/Superindustria-exige-a-edificios-y-conjuntos-residenciales-cumplir-con-normas-de-proteccion-de-datos-personales

Corte Constitucional colombiana, sala plena (Magistrado Ponente, Ciro Angarita Barón, 16 de junio de 1992) Sentencia No. T-414/92 https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

Corte Constitucional colombiana, sala plena (presidente, Jorge Arango Mejía, 1 de marzo de 1995) Sentencia No. SU-082/95. https://www.corteconstitucional.gov.co/relatoria/1995/su082-95.htm

Corte Constitucional colombiana, sala plena (Magistrado Ponente, Eduardo Montealegre Lynett, 5 de septiembre de 2002) Sentencia T-729/02 https://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm

Corte Constitucional colombiana, sala plena (Magistrado ponente, Juan Carlos Henao Pérez, 12 de mayo de 2010) Sentencia C-334/10 https://www.corteconstitucional.gov.co/relatoria/2010/C-334-10.htm

Corte Constitucional colombiana, sala plena (magistrada ponente, Adriana María Guillén Arango, 21 de junio de 2012). Sentencia SU458/12 https://www.corteconstitucional.gov.co/RELATORIA/2012/SU458-12.htm

Corte Constitucional colombiana, sala plena (magistrado ponente, Luis Ernesto Vargas Silva, 23 de noviembre de 2012). Sentencia T-987/12 https://www.corteconstitucional.gov.co/relatoria/2012/T-987-12.htm