UNIVERSIDAD MILITAR
NUEVA GRANADA

LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA FRENTE A LA NUEVA LEGISLACIÓN

:
Luz Alba Pinzón Franco

Monografía de grado

Director, Javier Francisco Franco Mongua
Abogado y Sociólogo. Magister en Derecho Económico

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE DERECHO
PREGRADO
BOGOTÀ
2013

LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA FRENTE A LA NUEVA LEGISLACIÓN

LUZ ALBA PINZÓN FRANCO

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE DERECHO
2013
BOGOTÁ D.C.

TABLA DE CONTENIDO

1. INTRODUCCIÓN.

El considerar la importancia y sensibilidad que tiene la información personal que se manipula a diario por los diferentes administradores tanto públicos como privados, nos invita a revisar si realmente se protegen adecuadamente los datos personales del individuo de conformidad con los derechos fundamentales que le han sido reconocidos, con la doctrina, la Ley y la jurisprudencia actual, en armonía con las políticas y procedimientos internos de cada Ente privado; aspectos que exigen una metodología de línea jurisprudencial y análisis estático, que se desarrolla en tres aspectos básicos, como son: (i) el escenario constitucional, base de los patrones facticos de conflicto a resolver por la Corte Constitucional; (ii) las sentencias hito, que permiten identificar y escoger conflictos a resolver de mayor o menor importancia doctrinal según la línea jurisprudencial escogida y, (iii) una relación de los pronunciamientos jurisprudenciales que son la estructura de interpretación de los diversos fallos sobre el tema jurídico, donde se analizan las reglas y subreglas propuestas para cada caso. Se usa esta metodología debido a que el desarrollo legal en Colombia es muy reciente y ha sido la jurisprudencia la vía por medio de la cual se han protegido los datos personales.

La importancia de la protección de la información personal surge como un imperativo de los negocios, en respuesta a las crecientes exigencias de los individuos cuya información personal es manejada dentro de los procesos de negocio de la Empresa, entendiéndose información personal

como toda aquella que se refiere a un individuo que pueda ser razonablemente relacionada con este y puede permitir su identificación. Cubre individuos que pueden ser empleados, relacionados con clientes, proveedores, contratistas, etc., y las relaciones pueden ser actuales, antiguas o prospectivas. Un incumplimiento puede afectar seriamente la reputación de la Empresa y exponerla a sanciones o multas por parte de los entes reguladores, originar una discriminación arbitraria o poner al individuo en riesgo grave. Es por ello que surge el cuestionarnos ¿Cuáles son las reglas de origen legal y jurisprudencial para la protección de los derechos fundamentales a la intimidad, al buen nombre, al habeas data y a la privacidad en Colombia, frente al manejo de la información personal en la empresa privada? A lo que se propone responder respetando la privacidad y la confidencialidad de los datos personales de nuestros clientes, mercado, reguladores y público en general que son procesados en los sistemas de información de la empresa privada de acuerdo con la legislación legal y jurisprudencial vigente e implementando los procesos a que haya lugar para su cumplimiento.

Se trata de un enfoque cualitativo, tiene una visión pragmática, se comprende la importancia de la protección de datos personales, se analiza el cuerpo normativo y la adopción de medidas para su cumplimiento; su alcance es descriptivo, con una temporalidad longitudinal ya que los datos son recogidos en diferentes tiempos y se utiliza una técnica documental. Para ello, se parte de los derechos fundamentales consagrados en el artículo 15 de la Constitución Política de 1991, se referencia como esos mismos derechos se han manejado en otros países, se efectúa un análisis legal y una línea jurisprudencial de la Corte Constitucional que evidencia el manejo dado en la actualidad.

El aporte de esta investigación, mostrará que el individuo tendrá acceso a su información personal sin restricciones; que la información personal que se maneje de él en bases de datos propagada por la tecnología va a estar protegida y regulada y, la necesidad de certificación de buenas prácticas en protección de datos personales.

Igualmente, ver al país seguro en la materia, evitar multas, cierres temporales o definitivos por incumplimiento, permitir a las empresas extranjeras realizar transferencias internacionales de información sin acudir al mecanismo de autorizaciones individuales. Para la industria de call centers y servicios tercerizados crear las condiciones ideales para el crecimiento y ser un fuerte motor de creación de empleo e inversión extranjera directa.

2. LA PROTECCIÓN DE DATOS PERSONALES DESDE LOS DERECHOS FUNDAMENTALES.

El reconocimiento a la protección de datos personales como un derecho fundamental se encuentra estipulado en el artículo 15 de la Constitución Política de Colombia, el cual establece:

> 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. (Gómez, 2009, p.19)

Esta norma constitucional no solamente ampara el derecho a la intimidad personal, sino familiar, la cual debe ser respetada por los demás; asimismo, protege el derecho al buen nombre, el habeas data, la libertad de información y la honra, derechos de los cuales hablaremos a continuación y donde el Estado es garante para protegerlos por medio de acciones judiciales como la acción de tutela, implementada con la finalidad de proteger los derechos fundamentales necesarios para que toda persona tenga una vida digna y acuda a su protección judicial en el evento en que estos sean objeto de violación o amenaza. Constituyen la condición de su libertad

y autodeterminación, son así mandatos de actuación y deberes de protección respaldados por el Estado.

2.1 DERECHO A LA INTIMIDAD.

Dentro de los derechos fundamentales, la Corte ha plasmado la norma específica que protege este derecho tanto para la persona como su familia, donde manifiesta que:

> La intimidad, es el espacio exclusivo de cada uno, es aquella órbita reservada para cada persona y de que toda persona debe gozar, que busca el aislamiento o inmunidad del individuo frente a la necesaria injerencia de los demás, dada la sociabilidad natural del ser humano. Es el área restringida inherente a toda persona o familia, que solamente puede ser penetrada por extraños con el consentimiento de su titular o mediando orden dictada por autoridad competente, en ejercicio de sus funciones y de conformidad con la Constitución y la ley. (C.Const., 1996, T-696, Morón Díaz, F.)

Es así como en el derecho a la intimidad prima el principio de la dignidad humana; la persona es autónoma en sus acciones, es quien escoge su espacio y lo limita a terceros; el Estado tiene el deber de respetarla y protegerla.

La Corte hace referencia a lo que se considera aspectos que pertenecen a la vida privada de una persona, como parte del derecho a la intimidad, los cuales son descritos como:

> a) ideas y creencias religiosas, filosóficas, mágicas y políticas que el individuo desee sustraer del conocimiento ajeno;
>
> b) aspectos concernientes a la vida amorosa y sexual;

c) aspectos no conocidos por extraños de la vida familiar, especialmente los de índole embarazosa para el individuo o para el grupo;

d) defectos o anomalías físicos o psíquicos no ostensibles;

e) comportamiento del sujeto que no es conocido de los extraños y que de ser conocido originaría críticas o desmejoraría la apreciación de éstos hacen de aquél;

f) afecciones de la salud cuyo conocimiento menoscabe el juicio que para fines sociales o profesionales formulan los demás acerca del sujeto;

g) contenido de comunicaciones escritas u orales de tipo personal, esto es, dirigidas únicamente para el conocimiento de una o más personas determinadas;

h) la vida pasada del sujeto, en cuanto pueda ser motivo de bochorno para éste;

i) orígenes familiares que lastimen la posición social y, en igual caso, cuestiones concernientes a la filiación y a los actos de Estado civil;

j) el cumplimiento de las funciones fisiológicas de excreción, y hechos o actos relativos al propio cuerpo que son tenidos por repugnantes o socialmente inaceptables (ruidos corporales, intromisión de dedos en cavidades naturales, etc.);

k) momentos penosos o de extremo abatimiento; y,

l) en general, todo dato, hecho o actividad personal no conocidos por otros, cuyo conocimiento por terceros produzca turbación moral o psíquica al afectado (desnudez, embarazo prematrimonial). Novoa (citado por C.Const., 1995, SU-089, Arango Mejía, J.)

Son descripciones propias del entorno del hombre, de su diario acontecer que lo centra en datos que conllevan a identificar a una persona, no siendo desde luego, todos de naturaleza íntima, pues parte de esa información personal se enmarca en la clasificación que la Corte ha designado como dato privado, semiprivado o público y su divulgación está garantizada constitucionalmente

en el Articulo 20 de la carta política, como otro derecho, el de la libertad de opinión, prensa e información.

Aquella información de tipo financiera y crediticia, ha sido calificada por la Corte Constitucional como semiprivada porque versa sobre información personal o impersonal, presenta para su acceso y conocimiento un grado mínimo de limitación, sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales, lo que significa que se halla por fuera de la esfera de la intimidad; es por ello, que encuentra desmedido colocar estas características propias de la intimidad personal y familiar en el mismo nivel del comportamiento crediticio de una persona. La Corporación fundamenta su argumento en dos aspectos: el primero, hace referencia a que es el deudor y sus acreedores existentes o futuros a quienes les interesa la deuda y, el segundo, muestra que se trata de una notoriedad de contenido económico no comparable con la vida, la libertad y la dignidad humana, aspectos que no tienen pertenencia con el derecho a la intimidad. (C.Const., 1995, SU-082, Arango Mejía. J.). Este tipo de información, siendo tan específica no tiene necesidad de invocar el derecho a la intimidad porque tiene naturaleza constitucional propia.

2.2 DERECHO AL BUEN NOMBRE.

El derecho al buen nombre es la apreciación que se tiene de una persona de acuerdo con las acciones y comportamiento que ejecuta dentro de la sociedad. Significa que:

(...) Hace referencia a la opinión o el concepto que sobre una persona tienen los demás, forma parte del patrimonio moral, es un componente de la dignidad humana, se gana con los propios actos, presupone que las conductas sean conocidas por los demás miembros de la sociedad, puede referirse a una actividad en particular como en lo que se desempeña una persona. (De la Calle, 2009, p.11)

Se trata entonces de las acciones propias que desarrolla como ser humano y la manera como llega a ser percibido en comunidad. La jurisprudencia Colombiana lo define como:

(...) El derecho al buen nombre es esencialmente un derecho de valor porque se construye por el merecimiento de la aceptación social, esto es, gira alrededor de la conducta que observe la persona en su desempeño dentro de la sociedad. La persona es juzgada por la sociedad que la rodea, la cual evalúa su comportamiento y sus actuaciones de acuerdo con unos patrones de admisión de conductas en el medio social y al calificar aquellos reconoce su proceder honesto y correcto. Por lo tanto, no es posible reclamar la protección al buen nombre cuando el comportamiento de la persona no le permite a los asociados considerarla como digna o acreedora de un buen concepto o estimación". (C.Const., 1995, SU-056, Barrera Carbonel, A.)

El comportamiento que tenga una persona en su entorno social es el factor relevante para el juzgamiento positivo o negativo de su fama, requiere que la información que se maneje de la persona sea completa, real, verídica y justificada para evitar que se vulnere su derecho.

2.3 DERECHO A LA HONRA.

Tal como ocurre con el buen nombre, se trata de un determinado comportamiento de la persona, teniendo presente el actuar, la ética y la compostura frente a la comunidad. La palabra honra se

relaciona con la estima y respeto que adquiere la persona por las virtudes y méritos propios, su afectación se da cuando, por ejemplo, existen motivos fundados en la comisión de un delito, se le acusa sin tener las pruebas que lo demuestren, esto daña su nombre y se incurre en una calumnia.

El concepto de honra tiene relación con la dignidad de la persona, concierne al espacio personal y se expresa en la pretensión de respeto individual. Si bien honra y honor pueden considerarse sinónimos, existe una diferencia clara entre los dos, la primera tiene que ver con el valor propio que tiene la persona de sí mismo sin interesar la opinión del mundo exterior, la segunda es el criterio que los demás tienen de ella. Igualmente, dentro de los fines esenciales del Estado Colombiano, el artículo 2 de la Constitución Política hace referencia a que las autoridades del país se encuentran constituidas para proteger a todos los residentes, en su vida, honra y bienes, creencias y demás derechos y libertades, con el fin de asegurar el cumplimiento de los deberes sociales del Estado y de los particulares. También, en el artículo 21 el Estado garantiza este derecho y la ley indicará cual es su forma de protección (Gómez, 2009).

Este derecho está consagrado el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, el cual establece que ninguna persona podrá ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, tampoco de ataques ilegales a su honra y reputación, la Ley lo protege contra estas irregularidades. (Oficina del Alto Comisionado para los Derechos Humanos (2007). De igual manera, la Convención Americana sobre Derechos Humanos (Pacto de San José) en su artículo 11 manifiesta que toda persona tiene

derecho al respeto de su honra y a que se le reconozca su dignidad, la ley la protegerá de tal manera que ninguna persona pueda ser centro de desacatos o abusos en su vida privada, la de su familia, en su domicilio, su correspondencia o ser víctima de ataques a su honra o reputación. Convención Americana sobre Derechos Humanos (Pacto de San José). En lo referente al aspecto penal, las conductas humanas que trasgredan el derecho a la honra están tipificadas como hechos punibles, bajo el título de delitos contra la integridad moral de la injuria y la calumnia (Código Penal Colombiano, 2009).

La legislación Colombiana, en muchas oportunidades se ha referido a este derecho explicando que se trata de un atributo esencial que tiene la persona, el cual, emana de su condición y dignidad. Es un bien jurídico personalísimo porque solo se predica de la persona en su condición de ser social, que se asemeja a otros derechos como la intimidad, buen nombre, habeas data y la protección de la correspondencia. Es el resultado de una valoración individual que hace a la persona merecedora de fe, confianza y credibilidad según su desempeño personal. (C.Const., 2002, T-494, Córdoba Triviño, J.).

2.4 DERECHO AL HABEAS DATA.

Este derecho, como lo ha manifestado reiteradamente la Corte Constitucional, consiste:

> (...) en la posibilidad que se otorga a toda persona para acudir a los bancos de datos y archivos de entidades públicas y privadas con el fin específico de demandar que le permitan el conocimiento, la actualización y la rectificación de las informaciones que hayan recogido acerca de ella. (C.Const., 1998, T-303, Hernández Galindo, J.)

Así como se le concede a la persona estas facultades explicitas, también lo faculta para que ella misma se encargue de vigilar si este amparo le llega ser vulnerado; para ello, la Corporación establece unas características, como son:

> (...) la información contenida en el archivo debe haber sido recogida de manera ilegal, sin el consentimiento del titular del dato (i), ser errónea (ii) o recaer sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente (iii). (C.Const., 1995, T-176, Cifuentes Muñoz, E.)

Esta descripción corresponde a situaciones en las que puede incurrir cualquier persona usuaria de un dato personal ajeno; de presentarse, configurarían violación a este derecho fundamental.

De la Calle (2009) considera que se presenta vulneración a este derecho fundamental, en todos aquellos casos en que se promueva una administración de información personal que atente contra los principios de administración de datos personales y las reglas fundamentales de origen legal que hacen referencia al tema. De esta manera, hay más precisión para definir los posibles eventos a ser considerados en la violación del derecho.

El Habeas Data en Colombia, de conformidad con la carta política, en su artículo 15, desglosa dos tipos, que son denominados el habeas data informativo y el habeas data correctivo, siendo el primero aquel que busca conseguir información sobre lo que se registró, el motivo, para quién se realizó y quién obtuvo los datos de ese registro; el segundo, tiene la finalidad de hallar lo que se encuentra incorrectamente registrado en una base de datos, para que la información sea corregida por su titular facultándolo para actualizarla o completarla (De la Calle, 2009). Se desprende así, una tipología que la jurisprudencia se encargó de garantizar y regular para el manejo de la

información contenida en bases de datos personales, especialmente aquellas relacionadas con la parte financiera, crediticia y comercial.

Este derecho comenzó como una garantía a la intimidad, luego como una revelación al libre desarrollo de la personalidad y, hoy en día, como el eje esencial que se encuentra conformado por la autodeterminación informática y la libertad, donde la persona tiene derecho a: 1) conocer la información que sobre ellas se tiene en las bases de datos; 2) incluir nuevos datos donde se registre una imagen completa del titular; 3) actualizar la información que se halla en los archivos; 4) que la información contenida sea rectificada y corregida; y 5) excluir información de una base de datos que sea indebidamente utilizada o por voluntad del titular, salvo las excepciones de ley. (C.Const., 2012, T-260, Sierra Porto, H.)

3. DATOS PERSONALES EN EL DERECHO COMPARADO

La protección que se busca dar a la información personal de los individuos, como derecho fundamental reconocido, no ha sido una práctica nueva; a través de la historia se han visto los diversos intentos por proteger la intimidad personal y darle un manejo adecuado a la información que de ella se recolecta y se almacena. Esta es la razón por la que diversos instrumentos internacionales, constituciones y legislaciones del mundo se han pronunciado a favor de este derecho, con el fin de garantizar y respetar los derechos fundamentales de las personas. A continuación se citan algunos.

3.1 ÁMBITO INTERNACIONAL.

En este entorno, algunas de las manifestaciones sobre la protección de datos personales son:

a) La Declaración Universal de los Derechos humanos de 1948: este documento adoptado por la Asamblea General de las Naciones Unidas, en el artículo 12, hace referencia a:

"Nadie será objeto de interferencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y a su reputación. Toda persona tiene derecho a la protección de la ley contra tales interferencias o ataques". (p.4). Se manifiesta expresamente la no intromisión en la vida personal del ciudadano y su familia otorgándole el derecho a su intimidad y privacidad.

b) La Declaración Americana de los derechos y deberes del hombre: afirma, en el artículo 5, que:

"(...) Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar" (p.2). La ley ampara la vida de la persona y la de su familia, al igual que le protege los derechos fundamentales a la honra y al buen nombre.

c) El Pacto Internacional de Derechos Civiles y políticos: el numeral 19.2 reconoce que:

"Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección" (p.3). Con este instrumento ya se empieza a reconocer expresamente el derecho a la información.

d) El Convenio para la Protección de los Derechos Humanos y las libertades Fundamentales: en el apartado 8.2, aprobó que:

> (...) No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás. (CPDHLF, 1950, p.10)

Los Estados firmantes del convenio serán los garantes en el otorgamiento de las restricciones y amparos de los derechos otorgados al ciudadano.

e) El Pacto de San José de Costa Rica, el numeral 14 estipula que:

1. Toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley.
2. En ningún caso la rectificación o la respuesta eximirán de las otras responsabilidades legales en que se hubiese incurrido.
3. Para la efectiva protección de la honra y la reputación, toda publicación o empresa periodística, cinematográfica, de radio o televisión tendrá una persona responsable que no esté protegida por inmunidades ni disponga de fuero especial. (PSJCR, 1969, p.3)

Con este pacto se reconoce el derecho y las libertades otorgadas a la personas para la protección de sus datos que reposan en bases de datos y se adoptan medidas para que puedan ser respondidos, rectificados y corregidos.

f) El Convenio 108 o Convenio de Estrasburgo: firmado en 1981 por Francia, Alemania, Dinamarca, Australia y Luxemburgo, está dirigido a garantizar el respeto de los derechos y libertades fundamentales de toda persona física, independientemente de su nacionalidad; en lo referente al manejo automatizado de sus datos, estos están clasificados como sensibles o

comunes, privados o públicos; el amparo se inicia desde el momento de entrar en vigencia el convenio; se trata de datos legítimos, legales y actualizados, garantiza los datos sensibles, el titular conoce de la existencia, fin, uso y actualización de su información. (Sánchez & Rojas, 2012).

3.2 CONTEXTOS LEGISLATIVOS.

La situación legal para la protección de datos en el mundo ha sido tema de muchos debates, uno de ellos se basa en analizarla desde dos modelos principales: el modelo europeo el cual busca que se proteja la información y la propiedad del titular, con el propósito de conservar la honorabilidad de la persona incluso cuando ésta hubiese fallecido; este modelo tiene base en los derechos humanos de los individuos. El modelo Estadounidense intenta proteger la información de las personas con el concepto de derecho a la privacidad, el cual consigue extinguirse con la muerte del individuo, el modelo nace derivado de motivos comerciales ya que las empresas utilizaban de manera indiscriminada esa información. (Sánchez & Rojas, 2012).

Así mismo, Oliveros (2011) considera que el modelo Europeo, cuya base es la protección de datos, se destaca el que tiene un enfoque preventivo, está socialmente orientado, hay confianza en el gobierno en cuanto a la cohesión y salvaguardias, los datos se adquieren cuando es necesario, los derechos y las excepciones se prevén en la ley, existen autoridades especializadas e independientes y se protege a toda persona que esté en territorio europeo. El modelo americano, para él, se basa en la privacidad, donde todo se resuelve en las cortes, tiene un

enfoque individual, confianza en el mercado, los datos se requieren sólo cuando son convenientes, los casos se resuelven uno a uno en las cortes, no existen autoridades concretas sino sectoriales, únicamente se protegen ciudadanos Estadounidenses. La tendencia que se observa es lograr que no se vulneren los derechos fundamentales del individuo y que se proteja su privacidad en todo su entorno. Urioste (1997) afirma, que la protección de datos personales puede presentar falsas apariencias respecto a su contenido, debido a que no tiene por objeto proteger los datos per se, sino una parte del derecho a la intimidad personal, aquella vinculada con la información individual. Los riegos percibidos en su almacenamiento y recopilación, se minimizaron con la evolución de la electrónica y la informática, pero no pueden estar ajenos a la política y al derecho. La evolución tecnológica, si bien aporta adelantos favorables en la recolección y almacenamiento de la información, también genera inseguridad en su custodia, vislumbrando una amenaza que el derecho a la intimidad podría sufrir por el uso descontrolado de las nuevas tecnologías. A nivel mundial, se ha buscado tener un respaldo jurídico para la protección de datos personales, tomando como base el desarrollo cultural, económico y político de cada país.

3.2.1 ALEMANIA.

Puccinelli (1999) reseña que el derecho a controlar los datos personales se inicia con la constitución de Weimar de 1919, la cual en su artículo 129 alude a reglas relativas al debido proceso en los procedimientos disciplinarios efectuados a los funcionarios públicos, allí se le

reconocían los derechos de acceso al expediente personal y que no se registrara información desfavorable sino hasta agotar la oportunidad de los descargos. El citado artículo reza:

> (...) La Ley regulará los haberes pasivos de funcionarios y sus familias. Los derechos adquiridos por los funcionarios son inviolables. Estos podrán acudir a la vía judicial para sus reclamaciones económicas. Sólo en los casos y en la forma previstos por la Ley, podrán los funcionarios ser suspendidos de empleo, separados del servicio provisional o definitivamente, o trasladados a otro cargo con remuneración inferior. Contra toda sanción disciplinaria cabrá recurso y habrá posibilidad de revisión. En el expediente personal del funcionario no se anotarán hechos que le sean desfavorables, sino después de haberle dado ocasión de manifestarse respecto a ellos. El funcionario tendrá derecho a examinar su expediente personal. La inviolabilidad de los derechos adquiridos y el acceso a la vía judicial para las reclamaciones económicas se garantizan también, de modo especial, a los militares profesionales. Su situación, por lo demás, será fijada por una Ley del Reich.

Con esta legislación se buscó respetar los derechos que la ley le otorgaba a la persona colocando un límite a los procedimientos legales.

Posteriormente, este mismo tratadista nos refiere a la primera ley consagrada específicamente a la regulación del tratamiento de datos personales, la Ley de Hesse, adoptada el 7 de octubre de 1970, la cual fue la primera en designar a un funcionario encargado de velar por el cumplimiento, protección y manejo de datos de los particulares. De aquí en adelante, las leyes sancionadas en Alemania que involucren el tema de protección de datos, se basan en el perfeccionamiento de lo ya existente, llenando los posibles vacios dejado por esta, mejorando la base legal de la

elaboración de datos, velando por los derechos del interesado y regulando los órganos de control para su protección.

3.2.2 PORTUGAL.

En 1976, Portugal fue el primer país europeo que reconoció constitucionalmente la necesitad de proteger a las personas frente a los riegos en el uso de la informática; con el pronunciamiento de la Ley 10 de 1991 se reglamento que debía gestionarse de forma transparente, donde rigurosamente se respetara la vida privada y familiar, los derechos, libertades y garantías fundamentales del ciudadano; se creó la autoridad responsable para su aplicación que sería la Comisión Nacional de Protección de Datos personales Informatizados; asimismo, se implantó que la información personal de las bases de datos era exclusiva del titular y se adoptó los principios del Convenio para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, promulgado por el Consejo de Europa. (Bazan, 2005). Esta legislación específicamente regula el tratamiento automatizado de la información personal que se tenga en las bases de datos, donde su manejo será conforme a las disposiciones de ley, con un fin determinado, pertinente, actualizado de tal forma que plenamente identifique al titular y garantice el tipo de información que se maneja. La constitución de la República Portuguesa ampara los derechos de los ciudadanos a acceder, rectificar, actualizar y conocer la finalidad a que se destinan sus datos, define el concepto de datos personales y su tratamiento, le da límites a la utilización de la informática, restringe el acceso de terceros a los datos personales, salvo aquellos previstos en la ley, prohíbe la atribución de un número nacional único, regula el

acceso a redes y flujos transfronterizos y protege los datos que se recolectan en ficheros manuales. (López, 2004). De esta manera se otorga el derecho a informarse sobre los contenidos de las bases de datos que le conciernen al titular de la información y el uso que se les pretende dar.

3.2.3 ESPAÑA.

Uno de los primeros países europeos en introducir en su legislación reglas para la protección de datos de los ciudadanos fue España, donde el Tribunal Constitucional aseveró que la regla amparaba un derecho fundamental autónomo que establecía una nueva garantía constitucional. (De la Calle, 2009). Es así como la Constitución Española de 1978, en su apartado 18.4 manifiesta que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Con esta promulgación, se limita el uso de los datos informáticos por los posibles riesgos en que se podría incurrir.

Al respecto, el Tribunal Constitucional Español reitera que se trata de un derecho independiente que se encuentra vinculado con la intimidad y que le permite a la persona el control, uso y destino de sus datos, evitando el riesgo de que tenga un uso diferente a aquel que se justificó en su recolección. El desarrollo de este derecho se encuentra enmarcado por:

g) El Convenio del Consejo de Europa del 28 de enero de 1981, para la protección de datos de carácter personal

h) La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (LORTAD)

i) La Directiva 95/46/CE, del Parlamento Europeo y del Consejo de 24 de octubre de 1995, referente a la protección de datos y libre circulación de los mismos (DOCE L 281, de 23 de noviembre de 1995), dio lugar a la redacción de una nueva ley, la L.O.15/1999, de 13 de diciembre, de protección de datos de carácter personal.

j) El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. (González & Moret, 2011).

Esta regulación permite a la persona el amparo de su información en bases de datos, teniendo acceso a su conocimiento, actualización, rectificación y un tratamiento especial de protección a los denominados datos sensibles, garantizando el reconocimiento a la autodeterminación informativa. Igualmente, se ocupa de los mecanismos a los que deben acomodarse las bases de datos personales.

El artículo 105.b del Estatuto Español de 1978, dispone que la ley regulará "El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas". Si bien la norma reconoce el derecho fundamental a la información, también expresa sus limitaciones para acceder a cierto tipo de datos reservados. Está excluido el acceso a los archivos y registros administrativos por parte de los ciudadanos cuando la información que contienen afecte la seguridad y defensa del Estado, revele delitos e intimidades de las personas, secreto comercial o industrial, se trate de temas de política monetaria, secretos oficiales, datos sanitarios personales

de los pacientes, datos del régimen electoral, datos estadísticos, registro civil y registro central de penados y rebeldes, datos de los representantes del gobierno. (González & Moret, 2011). La administración será garante del tipo de información que administre, teniendo presente los datos que por su naturaleza son clasificados como reservados. Velará por el estricto cumplimiento que la normatividad permite sin vulnerar el derecho amparado.

El artículo 20.4 del mismo Estatuto Español, dice que se reconocen y protegen los derechos.

> Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia. (Puccinelli, 1999, p.175).

Esto significa que los derechos fundamentales pueden ser sometidos a ciertas restricciones para salvaguardar la reputación o revelación de información confidencial, evento en el cual cada caso será analizado individualmente.

La constitución Española, interpreta la protección de datos frente al uso de la informática como un derecho independiente; le garantiza a la persona el control, uso y destino de los datos personales, con el fin de evitar un uso inapropiado que vulnere su dignidad y sus derechos. Le otorga la facultad al ciudadano para oponerse a que determinada información personal sea usada con fines distintos a aquel que requirió su obtención; intenta lograr una adecuación y exactitud de las bases de datos; brinda protección especial para datos sensibles; vela por el cumplimiento de la ley y establece un régimen sancionatorio. (González, 2011).

3.2.4 SUECIA.

Sobre la protección de datos en la Constitución de Suecia de 1974, podemos decir que en lo referente a las libertades y derechos fundamentales de los individuos, se garantiza que:

> Todo ciudadano estará salvaguardado contra cualquier autoridad que pretenda someterle a registro corporal o imponerle otro tipo de compulsión física, así como contra los registros domiciliarios o la intercepción de sus comunicaciones epistolares o telefónicas o la escucha clandestina de las mismas. (Carlos XVI Gustavo, 1974, p.2)

Se Garantiza la protección de los ciudadanos contra cualquier lesión de su integridad personal resultante del almacenamiento de datos que les afecten, mediante tratamiento informático. Asimismo, la inviolabilidad del domicilio y el secreto de las comunicaciones son centro de expresa divulgación. La Directiva Europea se introdujo en Suecia mediante la Ley de Datos Personales de 29 de abril de 1998. En ella, los apartados 48 y 49 estipulan los daños y las penas a aplicar. El artículo 48, implanta que el responsable de los datos personales indemnizará a la persona a la cual se le causaron los daños y por la violación de la integridad personal producida por el tratamiento de datos realizado ilícitamente, excepto que pruebe, que el error no fue causado por él, la obligación del pago de la indemnización se reduce o desaparece completamente. El artículo 49 castiga con multa o prisión hasta máximo de 6 meses, o de 2 años si la infracción es grave, a quien intencionadamente o por negligencia realice una de las conductas previstas en el citado precepto. Se trata de un sistema de días-multa en el que se establece la importancia o gravedad de la misma, no por una suma de dinero, sino por un número de días, según la gravedad del delito. Cada día equivale a una suma específica de dinero, según la posición económica del imputado. El título referente a los crímenes contra la libertad y la paz,

en su artículo 9c penaliza el incumplimiento del deber de secreto de datos personales con una multa la cual se encuentra regulada o con la pena de un máximo de dos años de prisión. Si hay tentativa, preparación o conspiración para cometer este delito también se castiga. (Bru, 2007). Esta legislación enfatiza el catalogo de ilícitos por los cuales se penaliza y multa al infractor y el reconocimiento de los derechos del titular solo lo contempla desde el punto de vista de la indemnización de perjuicios.

3.2.5 ESTADOS UNIDOS.

Para hablar de protección de datos en los Estados Unidos, debemos referirnos a la Ley de Libertad de información (Freedom of Information Act - FOIA), promulgada en 1966 la cual permite que la persona tenga derecho de acceder a la información del gobierno federal y de esta manera puede estar informado sobre su gobierno, se exceptúan aquellos archivos que son clasificados como información protegida para divulgación pública, expresamente señalada por la ley. (United States Department of Justice, 2011). Esta legislación le permite al ciudadano tener acceso a su propia información que se tenga almacenada en los registros de las agencias federales, entes públicos, limitando su consulta a los registros en poder de los órganos gubernamentales.

En 1970 fue aprobada una ley enfocada a proteger el manejo de la información relacionada al crédito, se trata de la Fair Creedit Reporting Act, la cual contiene presupuestos sobre los datos relativos a la solvencia patrimonial y el crédito, bajo el ideal de reglamentar el uso de una información que resulta fundamental para la actividad de la economía y el sistema bancario,

precedida de una administración proporcionada y respetuosa de la privacidad. (De la Calle, 2009). Su objetivo era proteger a los consumidores de competencias que afectaran su derecho a la privacidad y previniéndolos de un posible uso indebido por parte de las agencias recaudadoras de la información. Con el fin de reglamentar la recolección, mantenimiento, uso y difusión de la información de las personas que se mantiene en los sistemas de registros de los organismos federales, se crea la ley de protección de la vida privada, Privacy Act de 1974, una de las primeras protecciones frente al uso inadecuado de los datos personales por parte del gobierno, pero su alcance es restringido, ya que sólo se emplea en el procesamiento de datos por parte del gobierno federal, y no se aplica a los gobiernos estatales ni al sector privado. (Gregorio, 2004). Se observa entonces, que el sistema contempla una cobertura de protección para que se regulen los datos personales que reposan en documentos públicos.

Otras reglamentaciones estadunidenses que podemos mencionar son: la relacionada con el tratamiento de datos financieros, la Right to Financial Privacy Act de 1978, la cual hace referencia a los derechos de los clientes respecto de su información bancaria y la manera como estos datos pueden ser revelados a las agencias federales. Como regla general se exige el consentimiento del titular de la información, donde se encuentran varias excepciones, y la confidencialidad por parte de los administradores de la información. La Financial Modernization Services Act de 1999 (Billey Act-Gramm-Leach), la cual establece reglamentar el uso de la información personal construyendo políticas de información para el usuario. Los Safe Harbor Privacy Principles, principios de puerto seguro, instrumento que contiene las reglas que debe cumplir las entidades americanas para obtener la aprobación de la Unión Europea con

el fin de asegurar una política de protección de datos que brinde privacidad a un nivel equivalente al tipo europeo. (De la Calle, 2009). Todas estas son medidas tendientes a brindar protección al usuario frente a la información personal que de él se manejen en las diferentes bases de datos, pero su cobertura no es general si no que está sectorizada.

3.2.6 LATINOAMÈRICA.

Para América Latina, el surgimiento de las legislaciones sobre la protección de datos personales se origina de una necesidad por el aumento del uso de las tecnologías de la información y los posibles riegos. La generalidad de estas normas se asimiló al modelo europeo, tal es el caso de las leyes en Argentina, Chile, Panamá, Brasil, Paraguay, Uruguay. (Sánchez & Rojas, 2012). América Latina en materia de protección de datos ha evolucionado notoriamente, sancionando leyes generales en las que armoniza los lineamientos internacionales sobre la protección de datos personales y la legislación interna de cada país, con el objetivo de garantizar el derecho a la libertad y la privacidad de la información.

3.2.6.1 ARGENTINA.

La Ley 25.326, sancionada el 4 de octubre de 2000, ofrece un nivel de protección de datos personales avalado por la Comisión Europea como adecuado. Según la Decisión 2003/490/CE del 30 de junio de 2003, el órgano de control es la Dirección Nacional de Protección de Datos bajo el Ministerio de Justicia, Seguridad y Derechos Humanos. Esta ley, busca salvaguardar

integralmente los datos de carácter personal ubicados en registros o bancos de datos, con el fin de garantizar a las personas el derecho al honor, a la intimidad y controlar la información que sobre ellas se registre; exige un estricto código de conducta para la recolección y tratamiento de los datos; brinda especial protección a los datos sensibles. Precisa, una serie de obligaciones para quienes utilicen bases de datos con información personal; adopta medidas técnicas y organizativas que garanticen la seguridad y confidencialidad de los datos personales. (Sumer, 2010).

3.2.6.2 CHILE.

En Chile está la Ley 19.628 del 28 de agoto de 1999, sobre la protección de la vida privada. Es una legislativa general sin autoridad de control administrativa. La ley presenta unas insuficiencias que afectan la protección de los datos y la intimidad de las personas, como son: a) el carecer de un registro nacional de las bases de datos particulares existentes; los órganos públicos están obligados a registrar sus bases de datos en el servicio de registro civil, pero no existe sanción por su incumplimiento. b) no están definidas las infracciones a la ley y sus respectivas sanciones. c) no hay un órgano de fiscalización con facultades frente a organismos tanto públicos como privados, d) existe confusión en los conceptos de acceso público y encargado del tratamiento. (Ferrero, 2009).

3.2.6.3 PANAMÁ.

Hay un reconocimiento general explicito del derecho de Protección de Datos Personales y de Habeas Data. La Ley 6 de 22 de enero de 2002 dicta normas para la transparencia de la gestión pública, establece la acción del habeas data y otras disposiciones. Facilita el libre acceso a la información pública de todas las agencias o dependencias del Estado; Cuenta con el respaldo de varias organizaciones de la Sociedad Civil y de la Defensoría del Pueblo. La Ley 24 de 22 de mayo de 2002 regula el servicio de información sobre el historial del crédito de los consumidores o clientes.

3.2.6.4 URUGUAY.

Se encuentra la Ley 18.331 de protección de datos personales y acción de habeas data, del 11 de agosto 2008. Tiene como órgano de control a la Unidad Reguladora y de Control de Datos Personales, ente desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC). (Zamudio, 2012).

3.2.6.5 BRASIL.

La Constitución de Brasil de 1988, reglamenta que el habeas data se confiere para asegurar el conocimiento de informaciones relativas al peticionario, cuya información está en registros o bancos de datos de entidades gubernamentales o de carácter público, le da un amparo específico

permitiendo que pueda tener acceso a sus datos, rectificarlos y actualizarlos. Riascos (2009) refiere, que la constitución del estado federativo de Brasil regula la garantía constitucional de habeas data; la concede para asegurar el conocimiento de las informaciones relativas a la persona que se encuentra en los registros o bases de datos de entidades gubernamentales o de carácter público y le permite solicitar rectificación de los datos o informaciones que le conciernen.

3.2.6.6 PARAGUAY.

En el caso de Paraguay, la constitución de 1992, expresamente consagra la protección del habeas data y adiciona el amparo patrimonial y cobertura a los datos personales que se encuentren en registros o bancos de datos oficiales y privados. (Bazán, 2005). Esta legislación busca permanentemente velar en todo momento por la privacidad y confidencialidad de los datos personales que se encuentran en las bases de datos públicas y privadas, permite que los titulares sean conocedores del tratamiento, recolección, administración y actualización de la información.

3.2.6.7 MÉXICO.

En el caso Mexicano encontramos el pronunciamiento de Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, junto con el organismo fiscalizador de la misma, el Instituto Federal de Acceso a la Información y Protección de Datos. Entes encargados de la vigilancia de la Administración Pública Federal, el Instituto Federal Electoral (IFE), la Comisión Nacional de Derechos Humanos (CNDH) y el Banco de México.

Posteriormente, se consolidó la protección de datos personales en propiedad de las empresas particulares. Para ello, fue necesario efectuar modificaciones en la carta política Mexicana y reformar el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) para lograr un organismo público descentralizado de la Administración Pública Federal con autonomía operativa, presupuestaria y de decisión, y así como anuncia el 5 de julio de 2010 el decreto que expide la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), es de orden público y observancia general en todo el territorio Mexicano y su esencia es la protección de los datos personales en posesión de particulares para regular su tratamiento legítimo, informado y controlado para garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. (Oliveros, 2011). Con esta legislación se busca salvaguardar el respeto a la privacidad, dignidad e información de las personas, en ella se instituyen cuatro derechos fundamentales que tienen los individuos sobre su información en posesión de cualquier persona física o empresa particular (aseguradoras, bancos, tiendas departamentales, telefónicas, hospitales, laboratorios, universidades, etc.), son los llamados derechos ARCO: Acceso, Rectificación, Corrección y Oposición. Indica también, que los particulares deberán avisar, a cada persona de la que obtengan información personal, sobre el tratamiento que planean dar a sus datos, mediante un aviso de privacidad, el cual deberá ser respetado por el particular, y cada persona notificada tendrá la libertad de otorgar o no su consentimiento respecto al procesamiento de su información. (Sánchez & Rojas, 2012). Es así como el Estado establece obligaciones claras para todas las personas físicas o empresas que manejen bases de datos personales con el fin principal de que adopten medidas tendientes a

garantizar que dicha información estará adecuadamente protegida y no será objeto de un uso inadecuado.

3.2.6.8 COLOMBIA.

Las manifestaciones por proteger la información se revelan con el derecho consagrado en el Art.15 de la Carta Política de 1991, donde ampara que los datos personales sean manejados o administrados correctamente y bajo ciertos principios rectores. Posteriormente, se presentaron diversos proyectos no exitosos que se encargaron del tema, pero no cumplieron los requisitos que la constitución exige para las leyes que traten derechos fundamentales; En cuanto a las regulaciones, tenemos la Ley 510 de 1999 referente a las reglas en el sistema financiero y asegurador, y la ley 716 de 2001 acerca del saneamiento de la información contable en el sector público y otros temas tributarios, que fueron declarados inexequibles por la Corte Constitucional, porque no se tramitaron como leyes estatutarias, siendo requisito cuando de temas referentes a derechos fundamentales se trata. (Riascos, 2008). La Ley 1366 de 2008 ha sido establecida para desarrollar el derecho constitucional del habeas data. En la actualidad, la Ley Estatutaria 1581 de 2012, "Por el cual se dictan disposiciones generales para la protección de datos personales", pretende regular de una manera general el derecho fundamental a la protección de datos personales, expresado también como habeas data, o derecho a la autodeterminación informática o informativa, pero que se trata en realidad de aquel derecho que tienen todas las personas a ejercer las facultades de conocimiento, actualización y rectificación de la información personal que de ellas se contenga en bases de datos. Este régimen va a

permitir al titular de la información que su derecho a la intimidad y privacidad le sea respetado y tenga el control de la información personal que le corresponde.

El Decreto 1377 de 2013, "Por el cual se reglamenta parcialmente la Ley 1581 de 2012" tiene como objetivo reglamentar aspectos relacionados con la autorización del titular de la información, las políticas de los responsables y encargados, los derechos de los titulares de la información y la transferencia de los datos; reitera la importancia de los principios fundamentales para la recolección de datos personales relacionados con la finalidad y libertad, limitándolos a que sean solo aquellos pertinentes y adecuados al fin.

Como se observa, la iniciativa por encontrar un régimen de protección de datos personales en Colombia, tiene como esencia la protección de los derechos fundamentales del ciudadano, el cumplimiento de normas y la solución de conflictos motivados por la vulneración de derechos. Se trata de un sistema de salvaguarda donde lo que se busca "Es proveer una regulación que brinde una protección eficaz de los derechos fundamentales de las personas cuya información está o puede llegar a ser recogida, tratada o divulgada por un banco de datos, objetivo que se debe lograr sin llegar a eliminar o restringir severamente la utilización de dicha información para fines legítimos." (De la Calle, 2009, p. 129). Lo relevante aquí, es indicar las diferencias de régimen regulatorio que se le da a la información, según su naturaleza. La protección de los datos comprende normas y principios establecidos para su procesamiento en todas sus etapas como son la recolección, el almacenamiento, la circulación, la publicación, el uso, la divulgación y la transferencia nacional e internacional, los cuales se han incorporado por mandato

constitucional y local, representando una herramienta jurídica y un derecho fundamental frente al indebido o ilegal uso que le den los administradores y responsables.

4. ANÁLISIS EN LA LEGISLACIÓN COLOMBIANA Y SU REGLAMENTACIÓN

La Corte Constitucional, como garante de integridad y supremacía de la constitución, le hizo reiteradas invitaciones al Congreso de la República para que presentara y promoviera un proyecto de ley estatutaria que regulara la protección de los derechos relacionados con la libertad informática, habeas data y a la intimidad, hasta que finalmente lo alcanzó. En la actualidad, Colombia cuenta con una legislación desarrollada, solida e integral, que analizaremos a continuación, no sin antes hacer una breve reseña del marco conceptual del derecho a la protección de datos.

4.1 CONCEPTO DE DATO PERSONAL.

Por información personal se entiende cualquier dato o conjunto de datos que se relacionen con una persona y que sirvan para saber de quién se trata. La Ley define dato personal como "cualquier información vinculada o que pueda asociarse a una o varias personas naturales, determinadas o determinables" (Ley Estatutaria 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales". 17 de octubre de 2012). Aspecto que nos ubica con datos individuales. La Corte Constitucional en su sentencia T-022 de 1993 expresa que "por su manifiesta incidencia en la efectiva identificación o posibilidad de identificar a las personas, tal característica le confiere al dato una singular aptitud para afectar la intimidad de su titular mediante investigaciones o divulgaciones abusivas o indebidas". Esto nos lleva a que el dato habilita al receptor para que vincule la información con la persona. Si el

receptor accede a él en forma ilegítima, vulnera los derechos del titular de la información personal, como son la intimida, el buen nombre y el habeas data, entre otros.

4.2 CARACTERÍSTICAS.

La Corte definió cuatro características que describen lo que es un dato personal en la sentencia T-729 de 2002, y son los siguientes:

> "(...) i) el estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación".

Al estar frente a datos que se han identificado de una persona es ella la dueña de su información, es la titular de esos datos y su manejo estará regulado.

4.3 OBJETO.

Su estudio, como dice De la Calle, (2009, p. 145), comenzó por plantear un mecanismo para proteger al ciudadano de posibles excesos o errores que se encontraran en su información personal por mecanismos automatizados. Esta investigación fue financiada por el Congreso

Colombiano entre 1985 y 1986 y realizada por el CIFI (Centro de Investigaciones de las Facultades de Ingeniería y el CIJUS (Centro de Investigaciones Socio Jurídicas de la Facultad de Derecho de la Universidad de los Andes). Su resultado fue la presentación del proyecto de Ley 73 de 1986 "Por medio de la cual se crea el Estatuto para la Protección de la intimidad de las personas frente a los sistemas de información y los bancos de datos", proyecto que fue archivado por falta de elementos de juicio para pronunciarse a favor o en contra del mismo. Esto nos muestra que ya desde entonces se reflejaba la necesidad de encontrar un medio adecuado para proteger la información personal de posibles irregularidades.

4.4 INICIATIVAS DE PROTECCIÓN.

La exposición de motivos del Proyecto de Ley Estatutaria 1581 de 2012, se fundamenta en el desconocimiento que tiene el ciudadano sobre la finalidad para la cual sus datos personales son recolectados cuando accede a obtener bienes y servicios, ignora si son objeto de un uso adecuado o por el contrario se comercializan y circulan inapropiadamente; aspectos que hacen imperante una legislación integral y transversal para garantizar dicha protección desde el momento a partir del cual el titular da su consentimiento para su uso previamente conocido por él, hasta cuando sea manejada legítimamente por un tercero, contando con estándares de alta calidad y medidas concretas de protección. En Colombia, si bien se ha desarrollado normatividad sectorial para la protección de datos, esta no ha contemplado el avance integral del derecho al habeas data, evidenciando una falta de conexidad, pues ha sido la jurisprudencia de la Corte Constitucional la que a través de sus fallos de tutela ha delimitado su aplicación, fijando límites que permiten

diferenciarlo de otros derechos de igual categoría jurídica como el de la intimidad y libertad de información. Este proyecto, complementa la Ley 1266 de 2008, orientada especialmente al dato financiero y crediticio, pero que a su vez estableció las principales reglas y los principios aplicables a todo tipo de información personal; contempla el Convenio 108 de 1981 del Consejo de Europa, la Directiva Europea 95/46 de 1995, la Resolución 45/95 de 1990 de la ONU y la Resolución de Madrid de 2009, buscando con esto la acreditación de Colombia ante la Unión Europea como un país seguro en esta materia. (Congreso de Colombia. Exposición de Motivos Proyecto de Ley Estatutaria No.046 de 2010 Cámara).

Como se observa, la iniciativa por encontrar un régimen de protección de datos personales tiene como esencia la protección de los derechos fundamentales del ciudadano, el cumplimiento de normas y la solución de conflictos motivados por la vulneración de derechos. Se trata de un sistema de salvaguarda donde lo que se busca "Es proveer una regulación que brinde una protección eficaz de los derechos fundamentales de las personas cuya información está o puede llegar a ser recogida, tratada o divulgada por un banco de datos, objetivo que se debe lograr sin llegar a eliminar o restringir severamente la utilización de dicha información para fines legítimos." (De la Calle, 2009, p. 129).

4.5 LA INFORMACIÓN.

El tipo de información que se quiere proteger es aquella que, como la describe Puccinelli (2009, p.106-109), pudiera surgir de la relación entre datos, que logren la identificación del sujeto,

datos de personas físicas, aquellos vinculados a la publicidad que aunque en ocasiones son irrelevantes, pueden llegar a ser relacionados y procesados permitiendo descubrir aspectos que solo pueden circular con el consentimiento del titular. La protección es con el fin de evitar que terceros no autorizados accedan a la información sin causa justificada, que sean almacenados en sitios donde puedan ser tomados por personas distintas al registrador, se mantengan registrados de manera incorrecta o más del tiempo prudencial que corresponde, se conserven en la forma como se hallan registrados y no estén interconectados con otros, que no sean transferidos a otros sin autorización expresa del interesado o de la ley. En Colombia, la protección de datos desde el punto de vista del ordenamiento político y de las normas jurídicas ha tenido una intensa actividad a partir de su reconocimiento como derecho fundamental en la constitución política del 1991, disposiciones sectoriales y sus leyes estatutarias vigentes.

4.6 ADMINISTRACIÓN.

Para llevar a cabo el funcionamiento equilibrado y coherente de nuestra carta política, la Corte Constitucional se vale de principios jurídicos que garantizan el ejercicio de los derechos fundamentales de los usuarios, titulares de los datos y los administradores. Los entes responsables, tanto públicos como privados, ejecutan la administración de los datos personales bajo los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad, los cuales son base para el pronunciamiento de fallos y aporte a la doctrina constitucional como por ejemplo:

> Según el principio de libertad[1], los datos personales sólo pueden ser registrados y divulgados con el consentimiento[2] libre, previo y expreso del titular, de tal forma que se encuentra prohibida la obtención y divulgación de los mismos de manera ilícita[3] (ya sea sin la previa autorización del titular o en ausencia de mandato legal o judicial). En este sentido por ejemplo, se encuentra prohibida su enajenación o cesión por cualquier tipo contractual. (C.Const., 2002, T-729, Montealegre, E.)

El sustento del argumento es la necesidad de evitar el riesgo de que el poder informático pueda afectar derechos fundamentales del titular del dato, ya que su manejo ilícito sería un impedimento para estar en bancos de datos y circular.

El principio de necesidad, hace referencia a que el registro y la divulgación de los datos personales sean los estrictamente necesarios según el fin para el que sea requerido en la base de

---

[1] En la sentencia T-022 de 1993, la Corte resolvió el caso de la circulación de datos personales de contenido crediticio sin el consentimiento del titular de los datos. Es así como la Corte, bajo la necesidad de "favorecer una plena autodeterminación de la persona" y ante la "omisión de obtener la autorización expresa y escrita del titular para la circulación de sus datos económicos personales", resolvió conceder la tutela de los derechos a la intimidad y al debido proceso (léase propiamente *habeas data*) y ordenó a la central de información financiera el bloqueo de las datos personales del actor. Este principio encuentra su justificación, en la necesidad de evitar el riesgo que el poder informático entraña, en la medida que con el mismo se pueden afectar derechos fundamentales del titular del dato.

[2] Véase esta cualificación del consentimiento como libre, previo y expreso, en sentencia SU-082 de 1995 (consideraciones sexta y décima). Así mismo en sentencias T-097 de 1995, T-552 de 1997 T-527 de 2000 y T-578 de 2001.

[3] Sobre esta prohibición, a propósito de la interpretación del enunciado del artículo 15 de la Constitución y de la manera como se deben manejar los datos en relación con el principio de libertad, la Corte en la sentencia SU-028 de 1995, afirmó: "los datos conseguidos, por ejemplo, por medios ilícitos no pueden hacer parte de los bancos de datos y tampoco pueden circular. Obsérvese la referencia especial que la norma hace a la libertad, no sólo económica sino en todos los órdenes. Por esto, con razón se ha dicho que la libertad, referida no sólo al aspecto económico, hace parte del núcleo esencial del *habeas data*." En el mismo sentido en la Sentencia T-176 de 1995, consideró como una de las hipótesis de la vulneración del derecho al *habeas data* la recolección de la información "de manera ilegal, sin el consentimiento del titular de dato."

datos en que se encuentren; de lo contrario, al no existir una relación con el fin propuesto, se prohíbe.

En cuanto al principio de veracidad, los datos personales deben ser reales, verídicos, ya que está prohibida la administración de datos falsos o inexactos. De esta forma, se faculta al titular del dato personal para que acceda a su información positiva o negativa y la corrija total o parcialmente si esta no es real o le causa perjuicio.

La integridad, está muy relacionada con el principio de veracidad; lo que prevalece aquí es que la información personal del titular sea completa, que refleje la realidad de lo que se encuentra en la base de datos, se prohíbe el registro y divulgación de datos fraccionados o incompletos. El procesamiento, recolección y divulgación de los datos personales deben cumplir una finalidad legalmente justificada, en forma clara, suficiente y previa; de incumplirse este principio o darle un propósito diferente a su administración o delimitación, se prohíbe el manejo. La utilidad de la información personal, el acopio, procesamiento y divulgación deben cumplir con una determinada función, legitimando su derecho a la administración; el carecer de ella prohíbe la divulgación que no acata una utilidad clara o determinable.

Según el principio de circulación restringida, la divulgación y circulación de la información se halla sometida a los límites específicos determinados por el objeto de la base de datos, la autorización del titular y el principio de finalidad, de tal forma que queda prohibida la divulgación indiscriminada de los datos personales. De esta forma, se amparan los intereses del

ente que recibe la información confiada a él por el titular, si se trata de información pública o restringida, aspectos que de no ser motivados legítimamente para su solicitud, vulneran el derecho a la intimidad.

Según el principio de incorporación, cuando se agreguen datos personales en determinadas bases de datos que le brinden beneficios al titular, el ente administrador estará obligado a incorporarlos, previo al cumplimiento de los requisitos exigidos para ello. Respecto de la información negativa, desfavorable al titular del dato, el principio de caducidad establece que debe ser retirada de las bases de datos siguiendo criterios de razonabilidad y oportunidad, quedando prohibida la conservación indefinida de dicha información después de desaparecer las causas que dieron origen para ser incluida allí. De esta forma se protege al titular de la información de posibles injerencias indebidas en la libertad e intimidad, el abuso del poder informático y futuras privaciones de derechos.

Conforme al principio de individualidad y para proteger la libertad e intimidad del ciudadano, las administradoras deben mantener separadamente las bases de datos que se encuentren bajo su administración, se prohíbe facilitar cruce de datos a partir de la recolección de informaciones provenientes de diferentes bases de datos.

La Corte Constitucional manifiesta, que las obligaciones en la administración de bases de datos personales no se derivan únicamente de los principios rectores, si no que, existen otros como las

normas constitucionales y legales que tiene incidencia en el manejo de esta información y en la necesidad de indemnizar aquellos perjuicios causados por errores de la administración.

4.7 CLASIFICACIÓN DE LOS DATOS.

En la protección de datos personales, es imperante poder determinar claramente el tipo de información que se maneja, ya que estos nos lleva a conocer la libertad de circulación con la que se cuenta y la responsabilidad u obligación de los usuarios. En la sentencia T-729 de 2002, la Corte considera que se presenta una colisión entre el derecho al hábeas data o derecho a la autodeterminación informática y derecho a la información, con afectación algunas veces al derecho a la intimidad, situación que debe resolverse teniendo en cuenta la información de datos personales, los atributos y potestad del derecho a la autodeterminación.

Inicia su clasificación haciendo referencia a la información impersonal, en ella no existe un límite constitucional fuerte al derecho a la información, no habrá censura, está al servicio de los intereses generales y es de carácter público; colisiona con los derechos a la información, intimidad, al buen nombre y al habeas data. Luego habla de la información personal, refiriéndose a aquella contenida tanto en bases de datos computarizadas o no y la contenida en otros medios tales como videos, fotos. Posteriormente, la Sala encuentra desde su punto de vista cualitativo, cuatro clasificaciones: La información pública o de dominio público, esta no tiene reserva, puede ser general, privada o personal, acá encontramos los actos normativos de carácter general, los documentos públicos salvo los casos que establezca la ley, las providencias

judiciales ejecutoriadas, datos sobre el Estado civil de las personas o conformación familiar. La información semi-privada, versa sobre información personal o impersonal, tiene grado mínimo de limitación al ser obtenida y ofrecida por orden de autoridad administrativa, tales como datos de la seguridad social o comportamiento financiero. La información privada, contiene información personal o no, solo puede ser obtenida y ofrecida por orden de autoridad judicial; tal es el caso de los libros de los comerciantes, documentos privados, historias clínicas entre otros. La información reservada o secreta, es aquella personal que por su cercana relación con los derechos a la dignidad, intimidad y libertad del titular está reservada a su órbita exclusiva, como lo es la información genética, los datos sensibles, inclinación sexual, hábitos del individuo, etc. La ventaja de esta clasificación, observada por la Corte, es que delimita la información que se puede publicar y la que está prohibida como resultado de los derechos a la intimidad y habeas data, al igual que identifica quienes son los legitimados para su divulgación.

4.8 LEYES ESTATUTARIAS.

El Congreso las define como aquellas que la Constitución establece taxativamente, las cuales contienen una categoría superior respecto a las demás clases de leyes, debido a que tienen que surtir un trámite especial para su expedición debido a su importancia jurídica. Requiere mayoría absoluta y revisión previa por parte de la Corte Constitucional para su aprobación, entre ellas se encuentran las relacionadas con derechos y deberes fundamentales de las personas y los procedimientos y recursos para su efectiva protección.

El Congreso de la República de Colombia, el 17 de octubre de 2012, promulgó la Ley Estatutaria

1581 de 2012, "Por el cual se dictan disposiciones generales para la protección de datos personales", su objetivo principal, como lo considera la Corte en la sentencia C-748 de 2011, es regular de una manera general el derecho fundamental a la protección de datos personales, expresado también como habeas data, o derecho a la autodeterminación informática o informativa, pero que se trata en realidad de aquel derecho que tienen todas las personas a ejercer las facultades de conocimiento, actualización y rectificación de la información personal que de ellas se contenga en bases de datos. Este régimen va a permitir al titular de la información que su derecho a la intimidad y privacidad le sea respetado y tenga el control de la información personal que le corresponde. Su clasificación como ley estatutaria tiene una importancia especial, ya que, como lo dispone la carta política de 1991 en su Art. 152, a), los asuntos relacionados con derechos y deberes fundamentales de las personas y los procedimientos y recursos para su protección, son regulados mediante este tipo de leyes, las cuales deben cumplir con unos requisitos materiales y formales especiales.

Entre los objetivos que tiene la nueva Ley Estatutaria 1581 de 2012, están: i) proteger el derecho fundamental a conocer, actualizar y rectificar la información que se encuentre almacenada o recogida en bases de datos o archivos, ii) preservar el derecho a la intimidad, iii) amparar el derecho a la información. La Ley Estatutaria 1266 de 2008, cubre disposiciones generales del hábeas data, regula el manejo de la información contenida en bases de datos personales, especialmente la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y establece otras disposiciones. Hace énfasis únicamente en datos de carácter financiero y

comercial depositados en bancos de datos que se encuentran reportados en las centrales de riesgo.

En cuanto a los derechos desarrollados, la nueva ley regula unas categorías especiales de datos, con el fin de identificar qué información es la que requiere un trato específico por su naturaleza de sensible, ya que se puede afectar la intimidad de las personas o darle un uso inapropiado que genere discriminación. Asimismo, hace referencia al manejo de la información de los niños, niñas y adolescentes, a cómo es el entorno de legalidad para administrar la información de ellos, cómo sería la transferencia a otros países y las políticas corporativas que se manejen en el tratamiento de la información.

Respecto a las responsabilidades en el manejo de la información, la nueva reglamentación reparte las responsabilidades entre el responsable y el encargado del tratamiento de la información. La Ley 1266 de 2008, regula a cada uno de los implicados, determina claramente los compromisos para usuario y fuentes. Los derechos de que gozan los ciudadanos con la nueva normatividad son poder conocer, actualizar y rectificar sus datos personales, solicitar pruebas, ser informados referente al uso que se les va a dar, presentar quejas, revocar autorizaciones, solicitar supresión de los datos, todo esto dentro de los plazos establecidos para ello, al igual que poder acceder en forma gratuita a su consulta. La Ley 1266 de 2008 hace referencia a derechos frente a operadores de bancos de datos de información financiera en las centrales de riesgo.

Los mecanismo de vigilancia y control de protección de datos personales con la nueva Ley 1581 de 2012, se encuentran a cargo de la Superintendencia de Industria y Comercio, a través de una Delegatura de Protección de Datos. Se mantiene la vigilancia de los destinatarios de la ley 1266 de 2008, respecto a bases de datos personales destinados al cálculo de riesgo crediticio, a cargo de la Superintendencia financiera para operadores, fuentes y usuarios y se le otorga a la Superintendencia de Industria y Comercio la competencia residual.

La reglamentación actual, contempla algunas excepciones en las que la norma no tiene aplicabilidad, evitando así posibles conflictos entre derechos, como la libertad de expresión o la protección del orden público, y son ellas: las bases de datos o archivos personales o domésticos; las de datos financieros o crediticios reguladas por la Ley 1266 de 2008; las que tengan relación con temas de la defensa nacional, seguridad, prevención y control de lavado de activos, financiamiento del terrorismo; las bases de datos de inteligencia y contrainteligencia; las de contenidos editoriales y periodísticos; y, las del DANE, salvo que el titular de la información explícitamente lo haya autorizado, o se trate de una información de carácter médico prioritario, o esté relacionada con asuntos legales.

Para el Procedimiento de consultas y reclamaciones se mantiene lo ya establecido por la Ley 1266 de 2008, conservando el requisito de procedibilidad para formular quejas ante la Superintendencia de Industria y Comercio. Así el titular de la información o sus causahabientes pueden consultar por cualquier medio verbal o escrito y las reclamaciones las puede efectuar ante el operador o la fuente.

4.9 PARALELO DE PROTECCIÓN DE DATOS PERSONALES: LEYESVIGENTES

2008 LEY ESTATUTARIA 1266		2012 NUEVA LEY ESTATUTARIA 1581
OBJETO	Derecho a conocer, actualizar y rectificar la información recogida en bancos de datos. Recolección, tratamiento y circulación de datos personales (Art.15 C.N). Derecho a la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.	Derecho a conocer, actualizar y rectificar la información recogida en bases de datos o archivos. Derecho a la intimidad, habeas data, inviolabilidad de documentos privados (Art.15 C.N). Derecho a la información (Art.20 C.N.) Derecho a la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.
OBLIGACIONES	De los operadores, las fuentes y los usuarios de la información para garantizar el derecho del habeas data de petición, permitir el acceso de la información a los facultados para ello, adoptar un manual interno de políticas y procedimientos, solicitar certificación, conservar la seguridad de los registros almacenados y circular la información.	Del responsable y del encargado del tratamiento de la información, según sea su calidad deberá cumplir con garantizar al titular el derecho del habeas data, solicitar y conservar copia de la autorización otorgada por el titular, informar la finalidad del uso de la información recolectada, conservar la seguridad, veracidad, actualización, rectificación y privacidad de la información, adoptar un manual interno de políticas y procedimientos, tramitar las consultas y reclamos y cumplir con las instrucciones de la SIC.
DERECHOS CIUDADANOS	A la circulación de la información, de los derechos de los titulares a la información frente a los operadores de bancos de datos, fuentes de información y usuarios, de los deberes de estas mismas categorías de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.	A los datos sensibles, a la intimidad del titular, a los derechos de los niños, niñas y adolescentes, a los derechos y deberes de legalidad, la transferencia de datos a terceros países y las normas corporativas vinculantes.

2008 LEY ESTATUTARIA 1266		2012 NUEVA LEY ESTATUTARIA 1581
AUTORIDADES	Superintendencia de Industria y Comercio (vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países) y la Superintendencia Financiera de Colombia (En los casos en que la fuente, usuario u operador de información sea una entidad vigilada).	La Superintendencia de Industria y Comercio, a través de su delegatura para la protección de datos personales, en cabeza de un Superintendente delegado.
EXCEPCIONES	La información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley.	Las bases de datos o archivos personales o domésticos, aquellas que tenga finalidad la seguridad y la defensa Nacional , la prevención detección, monitoreo y control de lavado de activos y el financiamiento del terrorismo, bases de datos de inteligencia y contrainteligencia, bases de datos y archivos de información periodística y otros de contenido editoriales, bases de datos y archivos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y la Ley 79 de 1993 (censo de población y vivienda en el territorio Nacional).
PROCEDIMIENTOS	Peticiones, Consultas y Reclamos	Consultas, Reclamos y Requisito de procedibilidad.

4.10 REGLAMENTACIÓN.

La protección de datos personales en Colombia cuenta con varios sustentos vigentes como son: La Constitución Política de Colombia, la Ley Estatutaria 1266 de 2008, la sentencia C-1011 de 2008, el Decreto 1727 de 2009, el Decreto 2952 de 2010, la Ley Estatutaria 1581 de 2012, la Resolución 76434 de 2012 y el Decreto 1377 de 2013.

4.10.1 CONSTITUCIÓN POLÍTICA DE COLOMBIA.

En su Artículo 15 expresamente habla del derecho fundamental a conocer, actualizar y rectificar información que reposa en bases de datos tanto entidades públicas como privadas.

4.10.2 LEY ESTATUTARIA 1266 DE 2008.

Desarrolla disposiciones generales del hábeas data y su aplicación a todos los datos de información personal registrados en bases de datos de naturaleza pública o privada, especialmente la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

4.10.3 SENTENCIA C-1011 DE 2008.

Declaró exequible la Ley Estatutaria 1266 de 2008 que dicta disposiciones generales del habeas data y el manejo de datos contenidos en bases de datos personales, especialmente la financiera, crediticia, comercial, de servicios y de terceros países.

4.10.4 DECRETO 1727 DE 2009.

Determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.

4.10.5 DECRETO 2952 DE 2010.

Por el cual se regulan los artículos 12 y 13 de la Ley 1266 de 2008; hace precisiones sobre los requisitos especiales para fuentes de información y la permanencia de la misma.

4.10.6 LEY ESTATUTARIA 1581 DE 2012.

Dicta las disposiciones generales para la protección de datos personales registrados en cualquier base de datos susceptibles de tratamiento por entidades públicas o privadas.

4.10.7 RESOLUCIÒN 76434 DE 2012.

La cual deroga el contenido del título V de la Circular Única de la Superintendencia de Industria y Comercio, sobre Acreditación, y se imparten instrucciones relativas a la protección de datos personales, en particular, acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, las cuales se incorporan en el citado título.

4.10.8 DECRETO 1377 DE 2013.

Regula parcialmente la Ley 1581 de 2012, dicta las disposiciones generales sobre la protección de datos personales, favorece la inversión en el sector de servicios bajo estándares internacionales; protege derechos constitucionales tales como el habeas data, el buen nombre, la intimidad e información; establece límites adecuados en la recolección de los datos, fija el responsable del tratamiento y brinda seguridad en materia internacional.

5. LÍNEA JURISPRUDENCIAL DE LA CORTE CONSTITUCIONAL SOBRE PROTECCIÓN DE DATOS PERSONALES

5.1 PROBLEMA A RESOLVER.

Con el fin de construir la línea jurisprudencial se sigue la técnica propuesta por el tratadita Diego Eduardo López Medina, en su libro el Derecho de los Jueces. El tema que se analiza nos invita a plantear la siguiente pregunta: ¿Cuáles son las reglas de origen legal y jurisprudencial para la protección de los derechos fundamentales a la intimidad, buen nombre, habeas data y a la privacidad en Colombia, frente al manejo de la información personal en la empresa privada? La respuesta a este interrogante como lo ha expresado la Corte Constitucional, es que ante el acceso que se tiene a las bases de datos personales en la Internet y el fortalecimiento del poder informático, se han incrementado los riesgos de vulneración a los derechos como la intimidad, la libertad y la integridad personal, entre otros, esto debido a la ausencia de controles, inexistencia de reglas de protección sobre la materia, aspectos que reiteradamente la Corte ha manifestado a los entes reguladores se pronuncien, con el objeto de que promuevan y tramiten una regulación amplia e integral sobre la materia, bajo el supuesto de que la simple acción de tutela no es suficiente en el ámbito del poder informático.

¿Cuáles son las reglas de origen legal y jurisprudencial para la protección de los derechos fundamentales a la intimidad, al buen nombre, al habeas data y a la privacidad en Colombia, frente al manejo de la información personal en la empresa privada?

Ausencia de regulación reconociendo que la tutela es insuficiente en el manejo del ámbito del poder informático	• T-414/92 • SU-528/93 • SU-082/95 • **T-729/02** • C-1011/08 • C-334/10 • C-748/11 • SU-458/12	Necesidad de una regulación integral que proteja los derechos fundamentales en el ámbito del poder informático

5.2 SENTENCIAS SELECCIONADAS.

De los fallos emitidos por la Corte que dan respuesta a la pregunta planteada y que se relacionan con el tema de estudio, se escogieron las siguientes sentencias: T-414/92 que ilustra la desprotección en que hoy se encuentra el ciudadano colombiano frente a las entidades que organizan y administran bancos de datos, la SU-528/93 manifiesta que al hacer uso del mecanismo de acción de tutela por supuesta violación del Art.15 de la C.N.se debe acreditar la prescripción de la obligación, SU-082/95 evidencia que no hay vulneración de derechos fundamentales cuando existe autorización expresa y voluntaria por parte del actor, T-729/02 hay una deficiencia en las reglas de protección de derechos fundamentales relacionados con el manejo de las bases de datos y la necesidad de su medida, C-1011/08 protege el derecho al habeas data ante el abuso del poder informático, C-334/10 las medidas que afecten derechos fundamentales están sujeta a control judicial, C-748/11 reglamenta pautas generales para la protección de datos personales y SU-458/12 vulneración al derecho del habeas data.

5.3 PUNTO ARQUIMÉDICO.

Para graficar la línea jurisprudencial de los pronunciamientos anteriores, se toma la sentencia T-729/02 como el punto arquimédico de apoyo por ser el fallo más reciente sobre la materia y en el que la Corte Constitucional trata el tema de la regulación y el alcance del derecho al habeas data. Se observa en este estudio que esta Corporación a través de sus fallos ha conservado una posición constante, tendiente a unificar normas y jurisprudencia, buscando siempre la protección

del ciudadano en los eventos en que se vean afectados sus derechos fundamentales por las circunstancias actuales que se viven de orden público y de los avances tecnológicos a los que se ve enfrentado. Si bien esta corporación se ha pronunciado sobre el contenido y alcance del derecho constitucional del habeas data o la autodeterminación informática, los principios de la administración de las bases de datos, los datos personales y la clasificación de la información; advierte una deficiencia en los mecanismos de protección de derechos fundamentales relacionados con el manejo de las bases de datos y la necesidad de una regulación.

5.4 ANÀLISIS ESTÁTICO.

De las anteriores sentencias se procede a realizar el análisis estático donde se extrae la regla relacionada con el interrogante que se pretende resolver, correspondiendo al argumento principal en que se basa la Corporación para fallar y la subregla que apoya la decisión de la misma.

5.4.1 SENTENCIA: No. T-414 DE 16 DE JUNIO DE 1992.

Magistrado Ponente: Ciro Angarita Barón
Derechos Constitucionales Relacionados: Derecho a la Intimidad Personal y familiar, derecho a la información
Otros temas: Banco de datos, Dato Informático y habeas data

5.4.1.1 REGLA.

Se evidencia la desprotección en que se encuentra el ciudadano colombiano frente a las entidades que organizan y administran bancos de datos. La acción de tutela es un procedimiento para la protección inmediata de los derechos constitucionales fundamentales cuando éstos resulten vulnerados o amenazados por la acción o la omisión de la autoridad pública; igualmente, en la función pública de administrar justicia debe prevalecer el derecho sustancial y se observará la debida diligencia; entre los fines esenciales del Estado está el de garantizar la efectividad de los derechos consagrados en la Constitución, es el recurso efectivo que consagran los tratados y convenios internacionales para proteger eficazmente los derechos fundamentales. El otro medio de defensa judicial a disposición del reclamante ha de tener una efectividad igual o superior a la de la acción de tutela para lograr que sea efectiva e inmediata. No es suficiente con la existencia en abstracto de otro medio de defensa judicial si su eficacia es inferior a la de la acción de tutela.

5.4.1.2 SUBREGLA.

Se ha vulnerado el derecho a la intimidad, la libertad personal y la dignidad del reclamante mediante el abuso de la tecnología informática y del derecho a la información. La vulneración de tales derechos constitucionales fundamentales se materializa en la renuencia de la Asociación Bancaria de Colombia a cancelar su nombre de la lista de deudores morosos y actualizar

inmediatamente la información de su banco de datos computarizado, a sabiendas de que mediaba una sentencia ejecutoriada, el Juez declaró prescrita la obligación.

5.4.1.3 HECHOS.

El peticionario figura como deudor moroso del Banco de Bogotá en la Central de Información de la Asociación Bancaria de Colombia por razón de un crédito respaldado con un pagaré, el cual se vencía inicialmente el 14 de Julio de 1981 y fue prorrogado hasta el 14 de Noviembre de 1981. Por sentencia debidamente ejecutoriada, el Juzgado Décimo Sexto Civil del Circuito de Bogotá declaró prescrita la obligación del peticionario, el 27 de Abril de 1987. En los años 1988 y 1991 el peticionario personalmente y por intermedio de apoderado, solicitó a la Asociación Bancaria que lo retirara de la lista de deudores morosos, y esta entidad se negó acceder a su solicitud. Igualmente hizo la solicitud al Banco de Bogotá, y la rechazó verbalmente. El peticionario aparece como deudor moroso en el banco de datos de la Asociación Bancaria cuatro años después de ejecutoriada la sentencia que declaró extinguida su obligación.

5.4.1.4 CONSIDERACIONES.

La Corte reitera que en los actos de los encargados de administrar justicia debe prevalecer la categoría del ser sobre la del tener o del haber. En el presente caso se presentaron prácticas dilatorias en que incurrieron las autoridades competentes, el peticionario no dispone de otro medio de defensa judicial por lo que procede la acción de tutela incoada. Se ha vulnerado la

intimidad, la libertad personal y la dignidad del petente mediante el abuso de la tecnología informática y del derecho de y a la información. Se deben adoptar normas para el manejo de bases de datos y protección a la intimidad cuya atención deberá ser permanente. La vulneración de tales derechos constitucionales fundamentales se materializa en la renuencia de la Asociación Bancaria de Colombia a cancelar el nombre del peticionario de la lista de deudores morosos y actualizar inmediatamente la información de su banco de datos computarizado, conociendo que mediante sentencia ejecutoriada del 27 de abril de 1987, un Juez de la República declaró prescrita la obligación del peticionario con el Banco. La Corte reitera que ante un eventual conflicto, donde no haya un equilibrio entre el derecho a la información y el derecho a la intimidad, esta prevalece.

5.4.1.5 DECISIÓN.

Revocar la providencia del Tribunal Superior, ordenar la inmediata cancelación del nombre del peticionario de la lista de deudores morosos de la Central de Información de Asobancaria; Condenar a Asobancaria a la indemnizar del daño emergente, pagar las costas del proceso; solicitar al Consejo Superior de la Judicatura, El Tribunal Superior del Distrito Judicial y a la Procuraduría General de la Nación, presentar ante el Congreso de la República, un proyecto de ley que proteja eficazmente la intimidad y la libertad informática de los ciudadanos.

5.4.2 SENTENCIA: SU-528 DE 11 DE NOVIEMBRE DE 1993.

Magistrado Ponente: José Gregorio Hernández Galindo
Derechos Constitucionales Relacionados: Información, intimidad
Otros temas: acción de tutela improcedencia para declarar prescripción de la obligación

5.4.2.1 REGLA.

Se garantiza que toda persona, por el hecho de serlo, es titular a priori del derecho a su intimidad y el único legitimado para permitir la divulgación de los datos concernientes a su vida privada. Su titular no puede renunciar total o definitivamente a la intimidad pues dicho acto estaría viciado de nulidad absoluta.

Toda persona tiene derecho a informar y recibir información. Los bancos de datos funcionan en ejercicio de esta libertad. Cuando no existe motivo para la vinculación de los datos personales de un individuo al respectivo sistema informático, bien sea porque ya no existe la obligación que generó la inclusión, o por ser errónea o inexacta ésta, o por lesionar injustificadamente el buen nombre del peticionario, el dato debe ser retirado totalmente en cuanto a él atañe. Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo la cual impone a los responsables o administradores la obligación de una permanente actualización. Las informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia después de algún tiempo tales personas son titulares de un verdadero derecho al olvido.

En cuanto a la prescripción, se precisa que no es el juez de tutela el competente para declararla, por consiguiente esta no podrá ser alegada para dar por cancelado un dato informático si antes no se ha declarado la prescripción judicialmente. La tutela no es

procedimiento para declarar prescripciones, ya que esta materia corresponde a una jurisdicción distinta de la constitucional. Y si el juez de tutela carece de jurisdicción, tampoco tiene competencia.

5.4.2.2 SUBREGLA.

En casos de conflicto entre el derecho a la intimidad y el derecho a la información se reconoce la prevalencia del derecho a la intimidad por ser un elemento esencial de la personalidad y ser inescindible de la dignidad humana.

5.4.2.3 HECHOS.

Revisión de fallos proferidos por los Juzgados 47, 46 y 39 Civil Municipal de Bogotá, en acciones de tutela intentadas por el mismo peticionario contra distintas Instituciones Financieras. En el primer fallo, alega violación a la intimidad y al buen nombre porque figura reportado como deudor moroso en la central de información de las entidades demandadas por más de 10 años. Las pruebas allegadas evidencian que el peticionario no tiene claridad de qué entidad está cercenando su derecho, no hay daño por tanto tampoco perjuicio. En el segundo fallo se evidencia la vulneración del derecho a la intimidad ya que se encontraba prescrita la obligación y efectivamente no se procedió a retirarlo de la central como deudor moroso. El tercer fallo, subsume las demás tutelas presentadas por tratarse de los mismos supuestos facticos y porque todas encierran una conducta única. El Juez concluyó que la actividad del peticionario era

temeraria y, en consecuencia, además de rechazar la tutela, ordenó compulsar copias al juez penal competente. La decisión fue impugnada, pero, antes del fallo final, se desistió de la demanda.

5.4.2.4 CONSIDERACIONES.

La tutela no es el medio apto para declarar prescripciones. Aceptarlo involucraría prohijar la intervención indebida del juez de tutela en el campo reservado a otra jurisdicción. El peticionario admite en todos los casos que contrajo obligaciones con las entidades financieras contra las cuales dirige sus demandas, pero alega que tales obligaciones están prescritas y pretende que, se ordene el retiro de su nombre de los archivos y bancos de datos correspondientes. Considera la Corte que no es posible, pues en ninguno de dichos procesos se acreditada la prescripción judicialmente declarada. El habeas data busca defender a aquel contra quien se comete un acto contrario a la Constitución, no beneficiar a quien faltando a sus deberes, malversa la confianza de numerosas instituciones y aspira a un resarcimiento por un supuesto daño a su buen nombre.

5.4.2.5 DECISIÓN.

Confirmar las sentencias proferidas por el Juzgado 47 que niega la tutela impetrada por no existir violación al derecho fundamental aludido por el demandante; confirmar el fallo pronunciado por el Juzgado 39 que rechaza la tutela y ordena compulsar copias; revocar las sentencias proferidas por los juzgados 46 y 17.

5.4.3 SENTENCIA: SU-082 DE 1 DE MARZO DE 1995.

Magistrado Ponente: Jorge Arango Mejía
Derechos Constitucionales Relacionados: Derecho a la intimidad, Derecho al buen nombre y a la información
Otros temas: Habeas data, datos personales y las diversas clasificaciones de la información, límite temporal de la información

5.4.3.1 REGLA.

Para las facultades que otorga el Art. 15 de la carta política, es requisito necesario que la persona tenga conocimiento de la inclusión de su información en una base de datos y para ello, se requiere notificarla previamente y obtener su autorización libre y expresa, otorgada previamente al registro de la información de manera escrita.

5.4.3.2 SUBREGLA.

La información generada del comportamiento crediticio de las personas, no puede ampararse en el ámbito de protección del derecho a la intimidad, ya que la información relacionada con el manejo de una obligación crediticia no puede igualarse con la vida, la libertad y la dignidad del hombre. La protección al derecho del buen nombre solo la puede alegar quien lo tiene, ya que es

él quien propiamente lo adquirió, este prevalece frente al derecho a la información en caso de conflicto.

5.4.3.3 HECHOS.

El demandante solicitó en el año de 1990 un crédito a Invercrédito Servicios Financieros S.A. Por dificultades económicas se atrasó en los pagos del crédito, y fue reportado como deudor moroso a la División Datacredito, de la compañía Computec S.A. El demandante pagó su deuda, y le fue entregado el paz y salvo por la compañía que le otorgó el crédito. Sin embargo, su nombre aún aparece en el archivo de la demandada, con una anotación de "cartera recuperada", hecho que le ha impedido solicitar crédito o servir como garante de obligaciones contraídas por terceras personas. Solicitó ayuda a la Defensoría del Pueblo, Regional de Medellín, quien solicitó un informe a Invercrédito sobre el caso, y la respuesta fue la confirmación del crédito, sin saldo a la fecha y con un registro de mora de 120 días por lo que fue enviado a los abogados externos para cobro, reportándose como cartera recuperada.

5.4.3.4 CONSIDERACIONES.

La Corte se pregunta si ¿pertenece al ámbito de la intimidad de una persona la manera como responde por sus obligaciones económicas frente a las instituciones de crédito? La carta política en su Art. 15 ampara aquello que concierne solamente al individuo y a su esfera familiar, lo que allí acontece, es secreto, nadie extraño tiene por qué conocer cómo discurre la vida familiar, son

situaciones que pertenecen a la vida privada; por lo tanto, no se puede comparar en el mismo plano la intimidad con el comportamiento de una persona en materia crediticia, pues lo relacionado con el crédito y en especial la forma como él cumpla sus obligaciones, no pertenece a su intimidad.

Entra a establecer si se cumplieron las condiciones para que el demandante aparezca reportado ante las distintas centrales de información, siendo informada que al momento de solicitar el crédito y suscribir el pagaré el actor aceptó expresamente una cláusula de autorización a Invercredito para suministrar información a quienes tuvieren interés legitimo en ellas y que presentó una mora en el pago de su obligación hasta por cuatro meses, especificando que el crédito actualmente está pagado. Aún así, observa que esta información no es completa por lo que omite la fecha en que empezó la mora y el momento de su terminación, aspectos que revelarían el comportamiento comercial del demandante.

5.4.3.5 DECISIÒN.

Confirma parcialmente la decisión del Juzgado Veinte (20) Civil Municipal de Medellín, ordena a Datacrédito de Computec S.A., que en el término de las cuarenta y ocho horas Siguientes a la notificación del fallo agregue a los datos que posee sobre el comportamiento comercial del demandante la fecha en que él dejó de estar en mora con Invercrédito S.A., y que dicho crédito en la actualidad está totalmente cancelado.

5.4.4 SENTENCIA: No. T-729 DE 5 DE SEPTIEMBRE DE 2002.

Magistrado Ponente: Eduardo Montealegre Lynett
Derechos Constitucionales Relacionados: Derecho a la intimidad, derecho a la vida, la integridad personal, la propiedad y la libertad
Otros temas: Derecho constitucional al habeas data o a la autodeterminación informática, principios de la administración de las bases de datos, los datos personales y las diversas clasificaciones de la información, ausencia de regulación.

5.4.4.1 REGLA.

Se reconocen los principios que deben regir en toda administración de datos personales, como son el de libertad, necesidad, veracidad, integridad, finalidad, utilidad, circulación restringida, incorporación, caducidad e individualidad. Se clasifica la información en función de su publicidad como pública, semiprivada, privada y reservada; asimismo, la posibilidad legal de obtener acceso a ella.

5.4.4.2 SUBREGLA.

Se mencionan los principios de diligencia en el manejo de los datos personales y la obligación de indemnizar perjuicios causados por las posibles fallas en el proceso de la administración. Se sugiere la expedición de una regulación integral.

5.4.4.3 HECHOS.

El Departamento Administrativo de Catastro del Distrito capital, a partir del 2001 dispuso en Internet una página virtual con una base de datos sobre información catastral de Bogotá. Cualquier persona digitando el número de identificación puede obtener información como dirección, tipo de propiedad, área del terreno, área de construcción, etc, entre otros ítems, de los bienes inmuebles registrados en la base bajo ese número digitado. Se puede obtener información detallada del predio, tanto jurídica como económica con solo ingresar ciertos datos como matricula inmobiliaria, dirección, código del predial, cédula catastral y documento de identidad. Igualmente, la Superintendencia Nacional de Salud creó una página en Internet con una base de datos con la afiliación al régimen de seguridad social en salud, pudiendo cualquier persona con tan solo su identificación acceder al nombre completo del afiliado, fecha de afiliación, si presenta mora, los beneficiarios entre otros datos. Ante los hechos de violencia actuales como delincuencia común y grupos armados al margen de la ley, el actor ve vulnerado su derecho a la intimidad, a la vida y la de su familia, a la integridad personal, la propiedad y la libertad, por lo que instaura tutela siendo denegada por el Tribunal Superior de Distrito Judicial de Bogotá,

argumentando que la existencia de información en esas páginas no ponían en riesgo la integridad física del tutelante ya que son datos generales de la información de los usuarios para los fines que buscan dichas instituciones.

5.4.4.4 CONSIDERACIONES.

La sala considera que efectivamente se presenta tensión entre varios derechos fundamentales, desarrollados en el internet como comunicación global, no existiendo regulación para ello. Debido a la inobservancia y desconocimiento de los principios de libertad, finalidad e individualidad que son los que rigen la administración de datos personales, el Departamento Administrativo de Catastro del Distrito capital vulnera el derecho fundamental a la autodeterminación informática. Asimismo, la Superintendencia Nacional de Salud maneja datos catalogados como semi privados, lo que significa de acceso restringido, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en cumplimiento de sus funciones. El surgimiento del poder informático y el número único de identificación para los ciudadanos crea un factor de riesgo en el ejercicio de los derechos fundamentales, pudiendo de esta forma crear con la información recopilada en dichas bases de datos un "perfil virtual" de cualquier individuo, que afecta no solamente la autodeterminación informática, sino la intimidad, libertad e integridad física del individuo, riesgos que según la Corte son inevitables e irremediables mediante la acción de tutela, por lo que se hace necesario se expida una regulación integral al respecto.

5.4.4.5 DECISIÒN.

Revocar la sentencia proferida por la sala laboral del Tribunal Superior del Distrito Judicial de Bogotá, y a cambio conceder la tutela al derecho a la autodeterminación informática vulnerado por las entidades Departamento Administrativo de Catastro de Bogotá y la Superintendencia Nacional de Salud por la publicación de bases de datos en páginas de el Internet, a quienes se les ordena eliminar cualquier posibilidad de acceso indiscriminado, mediante la digitación de datos personales del actor. Promover que el Procurador General de la Nación y el Defensor del pueblo presenten un proyecto de ley estatutaria para la protección de los derechos fundamentales a la autodeterminación informática, habeas data, intimidad, libertad e información y que el Congreso de la República apruebe el respectivo proyecto presentado para la protección de estos derechos.

5.4.5 SENTENCIA: No. C-1011 DE 16 DE OCTUBRE DE 2008

Magistrado Ponente: Jaime Córdoba Triviño
Derechos Constitucionales Relacionados: Derecho al buen nombre, derecho de petición, derecho a la información, habeas data
Otros temas: Habeas data financiero, principios para la administración de datos personales

5.4.5.1 REGLA.

La temática del proyecto de ley está relacionada con la determinación de las reglas destinadas a regular el ejercicio del derecho a la autodeterminación informática o hábeas data de los titulares de información contenida en bases de datos personales, en especial aquellos datos de contenido financiero, crediticio, comercial, de servicios y la proveniente de terceros países. Cada uno de estos asuntos no sólo guarda relación estrecha con el núcleo temático del Proyecto de Ley, sino que toman la forma de herramientas necesarias para el desarrollo de los contenidos normativos propios de la regulación del derecho al hábeas data, específicamente en lo que respecta a la administración de datos personales de naturaleza financiera, comercial y crediticia. El ámbito de protección del derecho fundamental al hábeas data previsto en el Proyecto de Ley, se restringe a la administración de datos de índole comercial o financiera, destinada al cálculo del riesgo crediticio, con exclusión de otras modalidades de administración de datos personales. En relación con los mecanismos judiciales de defensa con que cuenta el titular de la información para la protección de su derecho fundamental al hábeas data, y para demandar justicia en relación con la obligación que se reporta como incumplida, ninguna objeción merece el hecho de que se prevea que la existencia de unos mecanismos directos no excluye la posibilidad de acceso a los medios de defensa judicial que contempla el orden jurídico en los ámbitos, constitucional y civil o comercial, en los términos previstos en los estatutos correspondientes.

5.4.5.2 SUBREGLA.

El hábeas data confiere un grupo de facultades al individuo para que, en ejercicio de la cláusula general de libertad, pueda controlar la información que de sí mismo ha sido recopilada por una central de información. En ese sentido, este derecho fundamental está dirigido a preservar los intereses del titular de la información ante el potencial abuso del poder informático, que para el caso particular ejercen las centrales de información financiera, destinada al cálculo del riesgo crediticio. Se restringe a limitar a un año la permanencia de la información financiera negativa a favor de determinados titulares que luego de pagar voluntariamente sus obligaciones, obtienen ese beneficio, de donde la fijación de términos especiales de caducidad del dato financiero negativo es un asunto intrínsecamente relacionado con el desarrollo de las facultades de conocimiento, actualización y rectificación del dato personal, las cuales integran el contenido esencial del derecho al hábeas data, de donde se concluye que el legislador estatutario estaba no sólo facultado para prever previsiones de esta naturaleza, sino que las mismas hacen parte de su competencia exclusiva, resultando desacertado considerar que la aplicación de la medida legislativa distorsione de tal manera el historial crediticio de los sujetos concernidos, de modo que tenga la virtualidad de amenazar la estabilidad del sistema financiero en su conjunto, como tampoco afecta desproporcionadamente el derecho de los usuarios a recibir información veraz e imparcial, pues simplemente reduce, más no elimina por completo, el término de caducidad en supuestos de hecho concretos y específicos, supeditados todos ellos al pago de las obligaciones en mora. Además, no se trata de una medida de aplicación sistemática, sino que opera por una sola vez, en los precisos términos dispuestos por el legislador estatutario.

5.4.5.3 HECHOS.

Se trata de la revisión de constitucionalidad del Proyecto de Ley Estatutaria 27 de 2006 Senado y 221 de 2007 Cámara, por la cual se dictan 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.

5.4.5.4 CONSIDERACIONES.

El proyecto de Ley busca desarrollar el derecho al buen nombre ya que no es pertinente que un ciudadano después de pagar su obligación en mora siga en las llamadas listas negras, limitándolo en sus operaciones comerciales, de esta forma se corrige el vicio procedimental que ejercen las centrales o bancos de datos. Asimismo, se busca el derecho de las personas a acceder a la información que se tiene de ellas en las bases de datos y archivos, rectificarla y actualizarla, hacer extensivo el derecho de petición a los organismos privados especialmente para las entidades financieras o bancarias y los bancos de datos.

5.4.5.5 DECISIÒN.

Por su aspecto formal, declarar exequible el proyecto de Ley Estatutaria 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. Declarar exequible el objeto, ámbito de aplicación, los principios de la administración de datos, los deberes de los operadores, fuentes y usuarios, el principio de favorecimiento a una actividad de interés público, los requisitos especiales tanto para operadores como para las fuentes, el acceso a la información por parte de los usuarios, las peticiones, consultas y reclamos, las sanciones y su criterio de graduación, el régimen de transición y su vigencia. El operador es responsable a partir de la recepción del dato suministrado por la fuente, por el incumplimiento de los deberes de diligencia, cuidado en la calidad de la información personal. Las entidades públicas del poder ejecutivo, cuando acceden al dato personal, se someten a los deberes y responsabilidades para los usuarios de la información. La fuente tiene la obligación de informar a los titulares los datos que suministra al operador. En caso de mora la caducidad del dato financiero inferior a dos años, no podrá exceder al doble de la mora y el término de permanencia de 4 años se contará a partir del momento en que por cualquier modo se extinga la obligación.

Las expresiones reporte negativo y reporte positivo hacen referencia al cumplimiento o incumplimiento de la obligación, el reporte deberá contener la información histórica, integral, objetiva y veraz del comportamiento crediticio del titular. Las Superintendencias en su función de vigilancia deben actuar con independencia y autonomía.

5.4.6 SENTENCIA: No. C-334 DE 12 DE MAYO DE 2010.

Magistrado Ponente: Juan Carlos Henao Pérez
Derechos Constitucionales Relacionados: Derecho a la intimidad, derecho a la honra, debido proceso, derecho a la información
Otros temas: Autodeterminación informática, datos personales públicos, privados, semiprivados y reservados

5.4.6.1 REGLA.

Las medidas de la Fiscalía que afecten derechos fundamentales requieren la respectiva autorización por parte del Juez de garantías. La intervención que la Fiscalía suponga en o los derechos fundamentales del sujeto de derecho, únicamente opera cuando sea indispensable y sólo en el grado que resulte plenamente justificado. El control judicial debe ser tenido en cuenta por el juez de garantías en los casos de allanamiento, registro, incautación, interceptación de comunicaciones, otra afectación a derechos fundamentales en la investigación del delito.

5.4.6.2 SUBREGLA.

La intervención que se haga sobre ámbitos del derecho a la intimidad de la persona misma, su familia u otros sujetos puede proceder pero sólo con la debida autorización judicial. El esperar a

que proceda la orden judicial previa no supone poner en riesgo el medio de prueba correspondiente y sí preserva los derechos fundamentales que se pueden afectar.

5.4.6. 3 HECHOS.

Un ciudadano considera que lo dispuesto en el Código de Procedimiento Penal, Art. 37, audiencia de control de legalidad posterior y Art. 245, examen de ADN que involucre al indagado o imputado, vulneran el derecho a la intimidad, el derecho a la honra, el debido proceso, al igual que las funciones de la fiscalía en asegurar los elementos materiales probatorios, garantizando la cadena de custodia mientras se ejerce su contradicción. Igualmente, el artículo 17, del Pacto Internacional de Derechos Civiles y Políticos, numeral 1, establece que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación; y el numeral 2, establece que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. Pues establece que no se contempla que el indagado o su defensor participen en la audiencia de control de garantías, analiza la ausencia de protocolos internacionales para el manejo de los datos personales en el proceso penal violando de esta forma los derechos fundamentales y humanos del procesado. Manifiesta que la legislación faculta a las personas a decidir cuáles datos quiere proporcionar bien sea al Estado o a un particular, que estos deben ser custodiados de tal forma que garantice el derecho al honor y a la intimidad de las personas así como el acceso a la información que se registre de ellas. Señala que la información dejada al navegar por internet u otros medios similares es inconstitucional, se puede acceder a información

confidencial en bases de datos, sin autorización judicial y sin que la medida se encuentre prevista en el numeral 2° del art. 250 CP. Sostiene que el acceso de la información contenida en ficheros clínicos o de salud, Art. 245 del Código de procedimiento penal, violan el derecho a la intimidad, toda vez que el acceso a tal información se debe someter a las mismas reglas que para la inspección corporal trae el artículo 247, porque en tales fichas se incluyen datos sensibles.

5.4.6.4 CONSIDERACIONES.

Sobre la ausencia de control de legalidad posterior, Art. 237 del CPP, resulta conforme a la Constitución que proceda un control judicial posterior a la actuación de la policía judicial tendiente a recuperar la información dejada al navegar en Internet u otros medios similares que aparecen en el computador incautado al indiciado, por estimar que tal actuación es una modalidad de registro, que se encuentra prevista dentro de las actuaciones de que trata el art. 250, numeral 2° de la Constitución política, disposición ya valorada en sentencia C-131 de 2009. Se analiza la constitucionalidad del precepto en lo que tiene que ver con el momento u oportunidad en el que debe operar el control judicial. Se reconocen en el Art. 250 del CP, la conservación de la prueba y la protección de los intereses generales y de la víctima. En el numeral 2°, establece la función de adelantar registros, allanamientos, incautaciones e interceptaciones de comunicaciones, sin contar con orden judicial previa, en las que el control del juez de garantías opera sólo dentro de las 36 horas siguientes a la actuación respectiva. El numeral 3°, reconoce la posibilidad de efectuar otras actuaciones distintas que en caso de afectación de derechos fundamentales, deben proceder siempre y cuando se obtenga la

autorización por parte del juez que ejerce las funciones de control de garantías. La cadena de custodia sobre las evidencias físicas y los elementos materiales probatorios recogidos por la Fiscalía, debe ser rigurosa y pueda ser útil durante el juicio, por legal, pertinente, ponderada. El cotejo de exámenes de ADN practicados anteriormente, con información genética del indiciado o imputado que reposa en bancos de sangre, esperma, laboratorios, consultorios médicos u odontológicos o similares, es una intervención no advertida dentro de los procedimientos de registro, allanamiento, incautación o interceptación de comunicaciones. No recae sobre bienes que sean de propiedad o que se encuentran bajo la tenencia del indicado o imputado, se realizan sobre muestras biológicas de éste, pero que se encuentran archivadas y custodiadas por centros especializados. En cuanto a la información clasificada como pública se entiende sin reserva y sin que se necesite autorización para ello. La semiprivada se requiere acceso por orden judicial o administrativa. La privada sólo por orden de autoridad judicial y la información reservada es aquella que solo interesa al titular, está relacionada con la protección de sus derechos a la dignidad humana la intimidad y la libertad.

5.4.6.5 DECISIÒN.

En lo que respecta al cargo formulado contra el art. 16, inciso 1° de la ley 1142 de 2007, por medio del cual se modificó el artículo 237, inciso 1° de la ley 906 de 2004, estarse a lo resuelto en la sentencia C-131 de 2009, Declarar exequible, en lo demandado, el artículo 42 de la Ley 610 de 2000. La defensa técnica en el proceso penal no tiene extensión a otros procesos y la presencia es obligatoria. La exigencia de ella como derecho fundamental ha sido circunscrita por

el constituyente al proceso penal ya que la responsabilidad penal involucra la afección directa de derechos fundamentales, circunstancia que conduce a que se intensifiquen al máximo las garantías contenidas en el debido proceso, pues se trata de dotar al ciudadano de las herramientas que requiera para colocarse en una situación de equilibrio ante el ejercicio del poder más drástico de que es titular el Estado. Declarar exequible por el cargo analizado, el inciso segundo del artículo 245 de la Ley 906 de 2004, excepto la expresión "dentro de las treinta y seis (36) horas siguientes a la terminación del examen respectivo, que se declara inexequible, en el entendido de que la revisión de legalidad que corresponde al juez de garantías, debe hacerse de manera previa.

5.4.7 SENTENCIA: No. C-748 DE 6 DE OCTUBRE DE 2011.

Magistrado Ponente: Jorge Ignacio Pretelt Chaljub
Derechos Constitucionales Relacionados: Derecho al Habeas data, derecho a la autodeterminación informática, derecho de los titulares de datos personales, derecho de petición
Otros temas: Información Pública, dato sensible, datos personales

5.4.7.1 REGLA.

El habeas data, identificado como un derecho fundamental autónomo tanto en el plano nacional como internacional, persigue la protección de los datos personales en un mundo 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 y el libre desarrollo de la personalidad. Sin embargo, el que exista una estrecha relación con tales derechos, no significa que no sea un derecho diferente, en tanto comprende una serie de garantías diferenciables y cuya protección es directamente reclamable por medio de la acción de tutela, sin prejuicio del principio de subsidiariedad que rige la procedencia de la acción. Sus ventajas mínimas son: (i) el derecho de las personas a conocer –acceso- la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a incluir nuevos datos con el fin de se provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa. El proyecto de ley regula en sus artículos 14 y 15 los mecanismos de consulta y reclamo del titular del dato o sus causahabientes al responsable o encargado del tratamiento.

5.4.7.2 SUBREGLA.

El habeas data como derecho fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben depender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de

derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones. El proyecto de ley estatutaria establece en materia de tratamiento de datos personales los principios de legalidad, el de finalidad, de libertad, de veracidad o calidad, de transparencia, de acceso y circulación restringida, de seguridad y el principio de confidencialidad, principios éstos que no obstan para que en el proceso de administración de bases de datos se dé aplicación a los principios rectores derivados directamente de la Constitución al igual que a aquellos derivados del núcleo temático del proyecto de ley estatutaria, los cuales pese a no encontrase numerados se entiende incorporados en razón de una lectura sistemática del proyecto de Ley Estatutaria.

5.4.7.3 HECHOS.

Control constitucional al Proyecto de Ley Estatutaria No. 184 de 2010 Senado; 046 de 2010 Cámara, por la cual se dictan disposiciones generales para la protección de datos personales.

5.4.7.4 CONSIDERACIONES.

La Corte considera que el trámite del proyecto de ley estatutaria cumplió los requisitos constitucionales para este tipo de leyes de especial jerarquía. Sin embargo, los Arts. 29, 30 y 31 relacionados con los datos relativos al certificado de antecedentes judiciales y el manejo de datos de inteligencia y contrainteligencia no cumplieron los principios de conectividad e identidad,

que consagra la obligación de que todos los asuntos aprobados en una ley hayan sido debatidos por las comisiones permanentes de ambas cámaras y por sus plenarias, estos no fueron objeto de los debates previos, fueron introducidos en el tercer y cuarto debates. Con este nuevo proyecto de ley se busca llenar el vacío de estándares mínimos de protección de todos los datos personales, el legislador ha dado paso a un sistema híbrido de protección en el que concurren una ley de principios generales con otras regulaciones sectoriales, que deben entenderse en conjunto con la ley general, pero que introduce reglas específicas para el tratamiento de cada tipo de dato. El contenido mínimo del derecho al habeas data lo constituye el derecho de las personas a conocer, accesar a la información que se tiene de ellas en las bases de datos, el derecho a incluir nuevos datos, el derecho a actualizarla, a que sea rectificada o corregida, a excluir información salvo las excepciones de ley. Señala que se prescindirá de la autorización cuando la información la requiera una autoridad pública o administrativa, sujeta a que esta entidad receptora cumpla con la obligación de protección y garantía bajo los principios de finalidad, utilidad y circulación restringida. Referente al suministro de información, cuando se trate de un dato sensible u de una niña, niño o adolescente, el responsable del tratamiento de la información deberá informar las limitaciones y derechos aplicables a este tipo de dato.

5.4.7.5 DECISIÒN.

En el aspecto formal declara exequible el proyecto de ley Estatutaria No. 046/10 de la Cámara y 184/10 del Senado, por el cual se dictan disposiciones generales para la protección de datos personales, los artículos 29, 30 y 31 se declaran inexequibles por vicios de procedimiento en su

aprobación. Los artículos referentes al objeto, ámbito de aplicación y definiciones, principios rectores, datos sensibles, derechos de los niños, niñas y adolescentes, autorización del titular, casos en que no es necesaria la autorización, suministro de información, deber de informar al titular, los procedimientos, los deberes de los responsables del tratamiento y encargados del tratamiento, tramite de procedimiento y sanciones, registro nacional de bases de datos, régimen de transición se declararon exequibles. El tratamiento de datos sensibles se declara exequible, excepto la frase que menciona que el titular haya hecho manifiestamente públicos los datos, pues considera que en actividades legítimas de un grupo de personas, sin ánimo de lucro, como las fundaciones, las ONG, las asociaciones, los sindicatos o cualquier otra, el hecho de pertenecer a dicho grupo no es razón para obviar la necesidad de obtener la autorización previa del titular de los datos. El derecho de los titulares, es exequible excepto la expresión *"solo"* que la declara inexequible ya que su entendimiento debe ser que el titular también podrá revocar la autorización y pedir la supresión del dato cuando no exista un deber de permanecer en dicha base de datos. La delegatura de protección de datos Personales deberá actuar de manera autónoma e independiente, entendida así, se declara exequible. Los recursos para el ejercicio de las funciones de la Superintendencia de Industria y Comercio se declaran exequibles, excepto por las multas que se impongan a los sometidos a vigilancia, porque contradice la prohibición de destinación de rentas específicas y el de unidad de caja establecido por el Estatuto Orgánico del Presupuesto Nacional, que es desarrollo de la Constitución económica. Por esto mismo en la parte de las sanciones, la expresión a favor de la Superintendencia de Industria y Comercio se declara inexequible. La prohibición de transferencia de datos personales se declara exequible, excepto por la expresión "necesaria" que se declara inexequible por considerarse que es abierta,

ambigua y general en el sentido de que no establece respecto de quien se reputa dicha necesidad, ni quien la define, ni cómo se establece. El Tratamiento sobre datos personales que requieran de disposiciones especiales se declara inexequible debido a que, si una norma legal requiere ser reglamentada para su debida ejecución e implementación, corresponde al Presidente de la República ejercer esa potestad sin que pueda otra autoridad dentro del Estado, como lo es la rama legislativa del poder público, fijarle términos para su ejercicio, por cuanto es una competencia permanente.

5.4.8 SENTENCIA: No. SU 458 DE 21DE JUNIO DE 2012

Magistrado Ponente: Adriana María Guillén Arango
Derechos Constitucionales Relacionados: Derecho a la intimidad, habeas data: finalidad, utilidad, necesidad y circulación restringida- información negativa- garantía
Otros temas: Dato personal, antecedentes penales,

5.4.8.1 REGLA.

La administración de bases de datos opera en contexto con el habeas data, su ejercicio es imposible jurídicamente en relación con información personal que no esté contenida en una base o banco de datos, o con información que no sea de carácter personal. La violación del derecho fundamental al habeas data vulnera otras garantías, como el derecho al trabajo y al buen nombre. El derecho al habeas data surge como una necesidad de establecer un cuerpo normativo singular

orientado a proteger las libertades individuales e igualmente como respuesta del constitucionalismo para enfrentar las amenazas a derechos fundamentales en que pueden incurrir las administradoras de las bases de datos por el robustecimiento de su poder informático. El principio de finalidad y sus pares, los principios de necesidad, utilidad y circulación restringida, tienen la intensión de limitar la actividad de administración de información personal contenida en bases de datos. Son principios que al limitar el ejercicio de las competencias de los administradores de bases de datos, definen el margen de su actuación y son una garantía para las libertades de los sujetos concernidos por la información administrada. El Ministerio de Defensa-Policía Nacional-, la Procuraduría General de la República, la Registraduría Nacional, la Fiscalía General, y la Unidad Administrativa Especial Migración Colombia tienen bajo su competencia la administración de bases de datos sobre antecedentes penales.

5.4.8.2 SUBREGLA.

La Corte señala que los antecedentes penales son considerados datos negativos; poseen el carácter de información pública; son producto de la imposición de una sanción, mas no una pena en sí misma; y se originan en la obligación constitucional de crear un banco de datos en el que se constate la existencia de hechos delictivos atribuibles a una persona. Asimismo, La facultad de supresión, como parte componente del habeas data, tiene una doble faz puesto que actúa de manera diferente frente a los distintos tiempos de la administración de información personal. En una primera faceta es posible ejercer la facultad de supresión con el fin de hacer desaparecer por completo de la base de datos la información personal respectiva, caso en el cual, la información

debe ser suprimida completamente y será imposible mantenerla o circularla, ni siquiera de forma restringida (esta es la idea original del llamado derecho al olvido). En una segunda faceta, la facultad de supresión puede ser ejercitada para hacer desaparecer la información que está sometida a circulación. Caso en el cual la información se suprime solo parcialmente, lo que implica todavía la posibilidad de almacenarla y de circularla, pero de forma especialmente restringida. Frente a la ausencia de reglamentación sobre el tema, se invita a la Defensoría del Pueblo, a la Procuraduría General y al Congreso de la República para que, en ejercicio de sus competencias, preparen un régimen aplicable a las bases de datos sobre antecedentes penales.

5.4.8.3 HECHOS.

Acciones de tutela instauradas por 13 actores, todas se refieren a un mismo problema jurídico contra el entonces Departamento Administrativo de Seguridad (en adelante DAS). Los demandantes fueron condenados por incurrir en algunos delitos consagrados en el CP, la autoridad judicial declaró la extensión de sus condenas o la prescripción de la pena. En pro de conseguir un trabajo o mantener el actual, solicitaron al DAS el certificado judicial de antecedentes judiciales, documento que fue expedido por dicha entidad con la leyenda "registra antecedentes, pero no es requerido por autoridad judicial". Se pidió formalmente al DAS por parte de algunos de los actores la eliminación de dicha anotación argumentando la extinción de la condena o la prescripción de la pena, peticiones que fueron absueltas de forma adversa. Consideran que se vulneraron sus derechos al habeas data, a la intimidad, al buen nombre, a la honra, a la igualdad, al debido proceso, al mínimo vital y al trabajo, ya que en el certificado no

debe aparecer que la persona registra antecedentes cuando la autoridad competente ha decretado la extinción o prescripción de la pena; el certificado no permite conocer el delito ni la fecha de condena; está divulgando la información de sus base de datos catalogada como reservada y solo disponible para una autoridad judicial cuando lo requiera; la permanencia de los antecedentes penales en el certificado judicial, aun cuando se ha decretado la extinción o la prescripción de la pena, equivale a una pena perpetua, al implicar la permanencia ilimitada de un dato adverso a la persona, viola el derecho al habeas data, causa discriminación en los ámbitos laboral y social, dificulta la reinserción social e impide acceder a un empleo digno.

5.4.8.4 CONSIDERACIONES.

La Corte establece que los antecedentes penales son datos personales, en la medida en que, asocian una situación determinada con una persona natural. Estos datos personales son propios y exclusivos de la persona, permiten identificarla, reconocerla individualmente o en conexión con otros datos personales. El habeas data para la Corte es un derecho de doble naturaleza, goza del reconocimiento constitucional de derecho autónomo, art. 15 C.N. y ha sido considerado como una garantía de otros derechos, especialmente los derechos a la intimidad, al buen nombre, a las libertades económicas y a la seguridad social, entre otros. El habeas data faculta al sujeto a conocer, actualizar, rectificar, autorizar, incluir y excluir su información personal cuando ésta es objeto de administración en una base de datos; tiene la función específica de proteger, mediante la vigilancia del cumplimiento de las reglas y principios de la administración de datos, los derechos y libertades que dependen o pueden ser afectados por una administración de datos

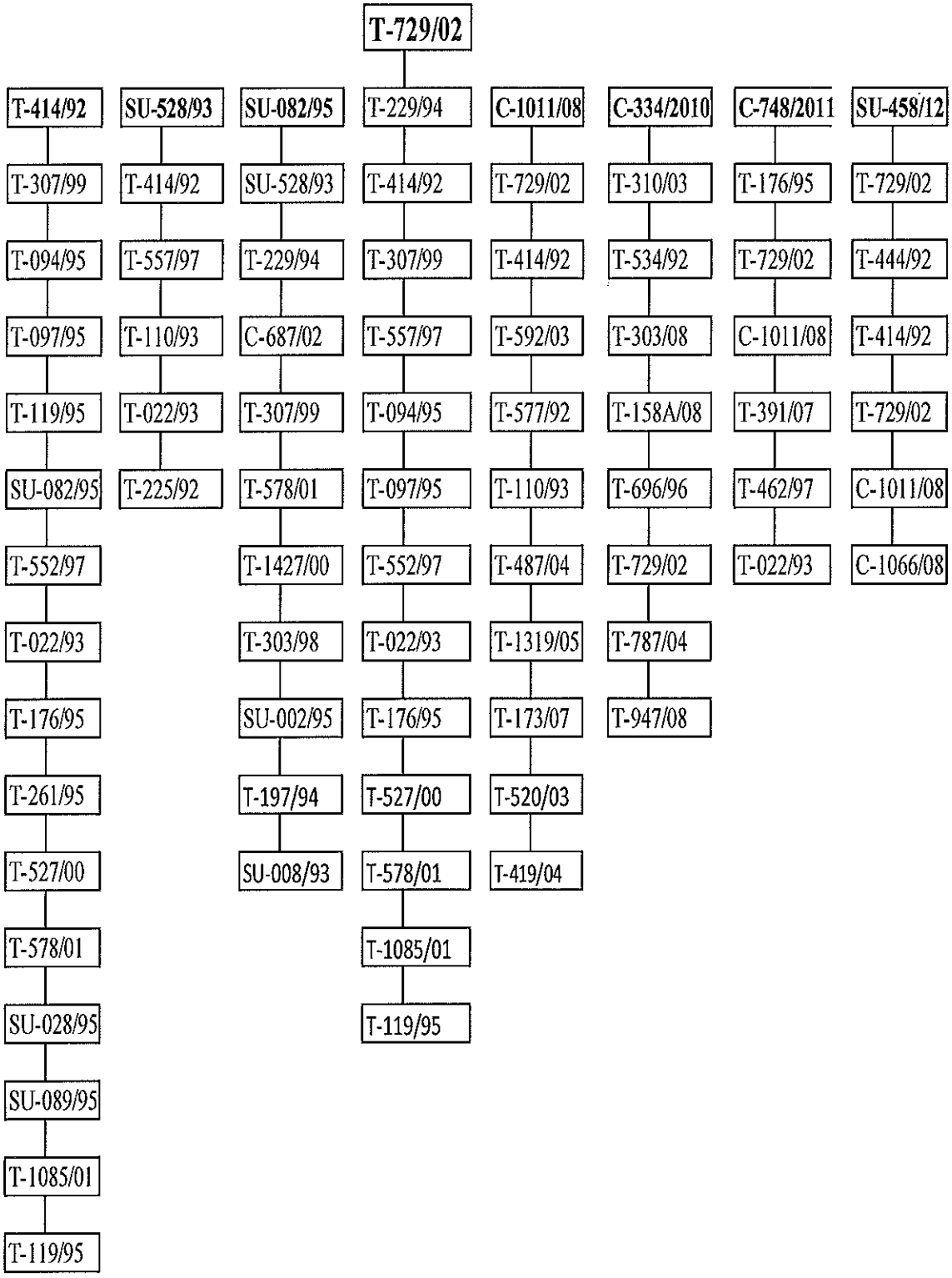
personales deficiente. La Corte consideró que la entidad encargada de administrar las bases de datos sobre antecedentes penales vulneró y vulnera aún el derecho al habeas data de los actores, al permitir que terceros no autorizados conozcan la existencia de antecedentes penales asociados a su nombre; esto se presenta por el desconocimiento de los principios de finalidad, necesidad, utilidad y circulación restringida de la información personal sobre antecedentes penales contenida en bases de datos y por la renuencia de la entidad a cargo de la administración de dicha base a suprimir dicha información, pese a una petición expresa de los actores para que terceros sin un interés previamente determinado conocieran dicha información.

5.4.8.5 DECISIÒN.

La Corte con el propósito de proteger el derecho fundamental al habeas data ordena al Ministerio de Defensa-Policía Nacional que para los casos de acceso a dicha información por parte de particulares, en especial, mediante el acceso a la base de datos en línea a través de las plataformas respectivas de la Internet, omita emplear cualquier fórmula que permita inferir la existencia de antecedentes penales en cabeza de los demandantes. Ordena a la Policía Nacional, - Dirección de Investigación Criminal e INTERPOL, que modifique el sistema de consulta en línea de antecedentes judiciales, de manera que al ingresar la cédula de los señores demandantes y de todos aquellos que se encuentren en una situación similar o que no registren antecedentes, aparezca la leyenda: "no tiene asuntos pendientes con las autoridades judiciales". Igualmente, con el fin de garantizar la vigencia de los principios de finalidad, utilidad, necesidad y circulación restringida de la información contenida en la base de datos personales sobre

antecedentes penales, pedirá que se modifique el sistema de consulta en línea de antecedentes judiciales, de manera que toda vez que terceros sin un interés legítimo, al ingresar el número de cédula de cualquier persona, registre o no antecedentes y siempre que no sea requerida por autoridad judicial, aparezca en la pantalla la leyenda "no tiene asuntos pendientes con las autoridades judiciales". La Sala es consciente de que exista ciertos escenarios concretos en los cuales algunos particulares precisan tener conocimiento sobre si alguien registra antecedentes penales o no, en estos casos, el deber de protección sumado a su interés, habilitarían a los particulares para exigir información suficiente en relación con la existencia o no de antecedentes penales. La Corte ha advertido la inexistencia de una regulación especial sobre las bases de datos de antecedentes penales, exhorta a la Defensoría del Pueblo, a la Procuraduría General y al Congreso de la República para que, en ejercicio de sus competencias, y si así lo estiman conveniente, prepare un proyecto de ley estatutaria en relación con el régimen aplicable a las bases de datos sobre antecedentes penales, que pueda atender los distintos intereses.

5.5 TELARAÑA NICHO JURISPRUDENCIAL.



6. CONCLUSIÓN

La empresa privada, en sus actividades cotidianas maneja una amplia gama de datos personales de sus clientes, mercado, reguladores y público en general, que hace imperante tener un debido cuidado frente al manejo de esta información; para ello, se requiere que el país cuente con una legislación integral que garantice la protección efectiva en el tratamiento de los datos personales; altos estándares de calidad, herramientas y medidas concretas para actuar, en caso de una posible vulneración a los derechos fundamentales reconocidos constitucionalmente.

Hasta el momento, la jurisprudencia de la Corte Constitucional es quien a través de sus fallos de tutela ha delimitado el ámbito de aplicación de la protección de datos personales. Desde la primera sentencia de tutela en 1992, la Corte reiteradamente ha manifestado la necesitad de una norma que proteja los derechos fundamentales en el ámbito del poder informático. Igualmente, reconoció que la tutela es un mecanismo constitucional insuficiente para ello.

Se evidencio, el hallazgo de una línea jurisprudencial formal, controlada y solida de la Corte Constitucional, donde demuestra a través de sus fallos que era la jurisprudencia la encargaba de proteger los datos personales, antes de existir la ley. Que hoy Colombia cuenta con un sistema hibrido de protección de datos personales con el que busca proteger la información, la propiedad y la privacidad de los datos personales.

La Ley 1266 de 2008, es la primera disposición de rango estatutario destinada exclusivamente a construir un sistema de protección de datos personales, su objeto es desarrollar el derecho

constitucional que tienen todas las personas a conocer, actualizar y rectificar informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales referidas en los artículos 15 y 20 de la constitución política de Colombia.

La Ley 1581 de 2012, complementa la regulación vigente para la protección del derecho fundamental de los ciudadanos a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación.

Este marco legal, permite que hoy Colombia cuente con las herramientas necesarias para brindar protección a los datos personales de los ciudadanos, obliga a las empresas a incorporar políticas de seguridad de protección de datos personales y ser cuidadosas al momento de su manejo; igualmente, a efectuar controles estrictos para cumplir con la normatividad.

El estudio de la línea jurisprudencial realizado, demuestra que los fallos de la Corte Constitucional evidencian reglas como: la acción de tutela como el mecanismo constitucional para reclamar la protección inmediata de los derechos fundamentales del ciudadano en el momento en que se vean vulnerados, los principios rectores que deben regir en el manejo de la información personal, el derecho al habeas data en el mundo globalizado y su importancia que deriva para otros derechos fundamentales, el derecho a conocer la inclusión de información en una base de datos y la autorización judicial para intervenir el ámbito de la intimidad personal o familiar, entre otras.

Dentro de las subreglas contempladas en las sentencias de la Corte Constitucional, podemos citar la prevalencia del derecho a la intimidad frente al derecho de información; el derecho al buen nombre frente al derecho de la información; la libertad personal, el derecho a la intimidad y a la dignidad humana frente al abuso de la tecnología. Así mismo, la indemnización por perjuicios, la supresión de datos negativos y una Institucionalidad administrativa que controle y vigile los procedimientos reglamentados.

La protección legal y jurisprudencial de la información personal, surge como una necesidad apremiante en respuesta a las crecientes exigencias de los individuos, cuya información personal es manejada dentro de los procesos de negocio de las empresas; por lo que se hace relevante, conocer los requisitos mínimos para su manejo los cuales se resumen así: unos principios fundamentales como son el procesamiento justo, la opción de oponerse, la exactitud para su proceso, la seguridad y acceso de la información, la transferencia a otros y su adherencia de cumplimiento. Así mismo, la creación de categorías de sujetos responsables del manejo, detallando sus deberes, requiriendo autorización previa del titular, definiendo las categorías de los datos, planteando excepciones y facultando a la Superintendencia de Industria y Comercio como la autoridad competente, bajo una delegatura, que garantice el cumplimiento de lo promulgado en la Ley y vele por la no transferencia de datos a terceros países que no cumplan con la adecuada protección de la información.

Cuenta así el ciudadano, con acceso a su información personal sin restricciones, la certificación de buenas prácticas en protección de datos personales, percibe al país seguro en la materia, evita

multas, cierres temporales o definitivos por incumplimiento, permite a las empresas extranjeras realizar transferencias internacionales de información sin acudir al mecanismo de autorizaciones individuales. Para la industria de call centers y servicios tercerizados, crea condiciones ideales para el crecimiento y es un fuerte motor de empleo e inversión extranjera directa.

7. REFERENCIAS.

Álvarez, M., Ávila, F.M. & Peñaranda H.R. (2000, 1 de enero) ¿Por qué la libertad informática constituye un nuevo derecho fundamental? Revista Internacional de Derecho e Informática. Recuperado de http://www.omdi.info/espanol/reivdi/ano2_n1/alvarez_2.htm

Bazan, V. (2005). *El habeas data y el derecho de autodeterminación informática en perspectiva de derecho comparado.* Estudios Constitucionales. Recuperado de http://www.cecoch.cl/docs/pdf/revista_ano3_2/revista_ano3_2_4.pdf

Bru, E, (2007, septiembre). La protección de datos en España y en la Unión Europea. Especial referencia a los jurídicos de reacción frente a la vulneración del derecho a la intimidad, *Revista de los Estudios de Derechos y ciencia Política de la UOC.* Recuperado de http://www.uoc.edu/idp/5/dt/esp/bru.pdf

Carlos XVI Gustavo.(1974). *Constitución de Suecia.* Recuperado de http://centros5.pntic.mec.es/ies.manuela.malasana/otros_servicios/ampliacion/ue25/suecia/suecia.pdf

Congreso de Colombia. Exposición de Motivos al Proyecto de Ley Estatutaria No.046. (2010) Cámara. *Por la cual se dictan disposiciones generales para la protección de datos personales.* Recuperado de http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/proyecto-de-ley-46-de-2010-camara.pdf

Convenio Europeo de Derechos Humanos (1950). *Convenio para la Protección de los Derechos Humanos y de la Libertades Fundamentales.* Recuperado de http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D800CBD20E595/0/Convention_SPA.pdf

Corte Constitucional Colombiana. Sentencia T-176 de 1995 (MP. Eduardo Cifuentes Muñoz; Abril 24 de 1995). Recuperado de http://www.corteconstitucional.gov.co/relatoria/1995/T-176-95.htm

Corte Constitucional Colombiana. Sentencia T-260 de 2012 (MP. Humberto Antonio Sierra Porto; Marzo 29 de 2012). Recuperado de http://www.corteconstitucional.gov.co/relatoria/2012/T-260-12.htm

Corte Constitucional Colombiana. Sentencia T-303 de 1998 (MP. José Gregorio Hernández; Junio 18 de 1998). Recuperado de http://www.corteconstitucional.gov.co/relatoria/1998/T-303-98.htm

Corte Constitucional Colombiana. Sentencia T-414 de 1992 (MP. Ciro Angarita Barón; Junio 16 de 1992). Recuperado de http://www.corteconstitucional.gov.co/relatoria/1992/T-414-92.htm

Corte Constitucional Colombiana. Sentencia T-437 de 2004 (MP. Clara Inés Vargas Hernández; Mayo 6 de 2004). Recuperado de http://www.corteconstitucional.gov.co/relatoria/2004/T-437-04.htm

Corte Constitucional de Colombia. Sala Novena. Sentencia T-987 de 2012 (MP. Luis Ernesto Vargas Silva; Noviembre 23 de 2012). Recuperado de http://www.corteconstitucional.gov.co/relatoria/2012/T-987-12.htm

Corte Constitucional de Colombia. Sala Plena. Sentencia C-1011 de 2008 (MP. Jaime Córdoba Triviño; Octubre 16 de 2008). Recuperado de http://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm

Corte Constitucional de Colombia. Sala Plena. Sentencia C-334 de 2010 (MP. Juan Carlos Henao Pérez; Mayo 12 de 2010). Recuperado de http://www.corteconstitucional.gov.co/relatoria/2010/C-334-10.htm

Corte Constitucional de Colombia. Sala Plena. Sentencia C-748 de 2011 (MP. Jorge Ignacio Pretelt Chaljub; Octubre 6 de 2011). Recuperado de http://www.corteconstitucional.gov.co/relatoria/2011/C-748-11.htm

Corte Constitucional de Colombia. Sala Plena. Sentencia SU-458 de 2012 (MP. Adriana María Guillén Arango; Junio 21 de 2012). Recuperado de http://www.corteconstitucional.gov.co/relatoria/2012/SU-458-12.htm

Corte Constitucional de Colombia. Sala Plena. Sentencia SU-528 de 1993 (MP. José Gregorio Hernández Galindo; Noviembre 11 de 1993). Recuperado de http://www.corteconstitucional.gov.co/relatoria/1993/SU-528-93.htm

Corte Constitucional de Colombia. Sala Primera de Revisión. Sentencia SU-082 de 1995 (MP. Jorge Arango Mejía; Marzo 1 de 1995). Recuperado de http://www.corteconstitucional.gov.co/relatoria/1995/SU-082-95.htm

Corte Constitucional de Colombia. Sala Séptima de Revisión. Sentencia T-729 de 2002 (MP. Eduardo Montealegre Lynett; Septiembre 5 de 2002). Recuperado de http://www.corteconstitucional.gov.co/relatoria/2002/T-729-02.htm

Corte Constitucional de Colombia. Sentencia SU-056 de 1995 (MP. Antonio Barrera Carbonel; Febrero 16 de 1995). Recuperado de http://www.corteconstitucional.gov.co/relatoria/1995/SU-056-95.htm

Corte Constitucional de Colombia. Sentencia SU-089 de 1995 (MP. Jorge Arango Mejía; Marzo 1 de 1995). Recuperado de http://www.corteconstitucional.gov.co/relatoria/1995/SU-089-95.htm

De la Calle, J.M. (Ed.). (2009) *Autodeterminación Informativa y habeas Data en Colombia.* Bogotá D.C.: Editorial Temis S.A. p.43, 54, 55.

Departamento de Derecho Internacional (1969). *Convención Americana sobre Derechos Humanos (Pacto de San José)* Recuperado de http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

Ferrero, A. (2009). Consejo para la Transparencia. *Estrategias Emergentes para el Desarrollo de la Protección de datos en Chile.* Recuperado de http://www.redipd.org/actividades/encuentros/VII/common/alejandro_ferrero_chile.pdf

Gómez, F. (2009). Constitución Política de Colombia Anotada. Bogotá: Editorial Leyer

González, A. & Moret V. (2011). Constitución Española. *De los Derechos y Deberes Fundamentales Sinopsis Articulo 18 - Informática.* Recuperado de http://www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=10&fin=55&tipo=2

Gregorio, C.G. (2004). Protección de Datos Personales: *Europa vs. Estados Unidos, Todo un Dilema para América Latina.* Recuperado de http://biblio.juridicas.unam.mx/libros/3/1407/12.pdf

Ley No. 6 de 22 de enero de 2002. Que dicta normas para la transferencia en la gestión pública, establece la acción de Habeas Data y otras disposiciones. Recuperado de http://www.redipd.org/legislacion/common/legislacion/panama/ley_num_6.pdf

Ley No. 24 de 22 de mayo de 2002. Que regula el servicio de información sobre el historial del crédito de los consumidores o clientes. Recuperado de http://www.legalinfo-panama.com/legislación/00297.pdf

Ley Estatutaria 1286 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. 31de diciembre de 2008. DO.N°47.219.

Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 17 de octubre de 2012. DO.N°48.587.

López, D.E. (Ed). (2012). *El Derecho de los Jueces.* Bogotá: Legis Editores.

López, D.A. (2004). Observatorio Iberoamericano de Protección de Datos - Portugal. Revista Digital Datospersonales.org. Recuperado de http://oiprodat.com/normativa-y-legislacion/portugal/

Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio (2012). Resolución Número 76434 de 2012. Recuperado de http://www.sic.gov.co/documents/10157/353524/Resolucion_76434_2012.pdf/a757d909-3a7e-49a3-a172-71ef0d55d238.

Ministerio de Hacienda y Crédito Público (2009). Decreto Número 1727 de 2009. Recuperado de http://www.sic.gov.co/documents/10157/1557222/Decreto_1727_2009.pdf/7ebc2ce2-516d-4d4e-94a2-5a4f8744c022

Ministerio de Hacienda y Crédito Público (2010). Decreto Número 2952 de 2010. Recuperado de http://www.sic.gov.co/recursos_user/documentos/normatividad/Decreto_2952_2010.pdf

Novoa, E. (1979) Derecho a la Vida Privada y Libertad de Información. México: Siglo XIX Editores. p.45, 46.

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (1966). *Pacto Internacional de Derechos Civiles y Políticos.* Recuperado de http://www2.ohchr.org/spanish/law/ccpr.htm

Oliveros, A, (2011, enero). Ley Federal de Protección de Datos Personales en Posesión de Particulares, *MAGAZCITUM el Magazine para los Profesionales de TI,* (2), Recuperado de http://www.uoc.edu/idp/5/dt/esp/bru.pdf

Organización de los Estados Americanos (1948). Documentos Básicos. Comisión Interamericana de Derechos Humanos. *Declaración Americana de los Derechos y deberes del Hombre.* Recuperado de http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp

Puccinelli, O. (Ed.). (1999) *El habeas Data en Iberoamérica.* Bogotá D.C.: Editorial Temis S.A. p.139.

Riascos, L. (2008). El Hábeas data en algunos proyectos de Ley Estatutaria en el derecho Colombiano. Extraído Marzo 26, 2013, desde http://www.derecom.com/revista/num0608/pdf/HABEAS_DATA_COLOMBIA.pdf.

Riascos, L. (2009, 25 de abril). La Visión Constitucional del Habeas Data. *Revista Informática Jurídica.* Recuperado de http://www.informatica-juridica.com/trabajos/La_vision_constitucional_del_habeas_data.asp

Sánchez, G., & Rojas, I. (2012). Leyes de Protección de Datos en el Mundo y la Protección de Datos biométricos - Parte 1. *Seguridad Cultura de Prevención para TI, volumen (13),* 6-7. Recuperado de http://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93

Sumer, M. (2010). Informática Legal. *La Protección de datos personales en Argentina.* Recuperado de http://www.informaticalegal.com.ar/2010/03/16/la-proteccion-de-datos-personales-en-argentina/

United State Department of Justice (2011). *FOIA.Gov.* Recuperado de http://www.foia.gov/index-es.html

Urioste, M., (1997). Protección de Datos Personales. Fundación para el Estudio y Difusión del Derecho Comparado. Recuperado de http://www.derecho-comparado.org/newsletter/Nws18.html

Zamudio, M, (2012, Jul-Dic). El Marco Normativo Latinoamericano y la Ley de Protección de Datos Personales del Perú, *Revista Internacional de Protección de Datos Personales*, 1, 7. Recuperado de http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok3_Ma.-de-Lourdes-Zamudio_FINAL.pdf

8. ANEXOS

PROYECTO		ASUNTO	OBSERVACIÒN
LEY 070 DE 1997	CAMARA	Intimidad personal, el buen nombre frente a los sistemas de información y bancos de datos, se crea la Comisión Protectora de Bancos de Datos. (Gaceta del Congreso No.376 Sept.16/97)	
LEY ESTATUTARIA 115 DE 1997	SENADO	Se protegen la intimidad, el hábeas data y el buen nombre mediante la regulación del tratamiento y uso de datos personales.(Gaceta del Congreso No.437 Oct.20/97)	
LEY ESTATUTARIA 52 DE 2000	SENADO	Se regula el ejercicio de los derechos al hábeas data, la información, tratamiento de información financiera y comercial en bases de datos.(Gaceta del Congreso No.317 Agt.10/00	
LEY ESTATUTARIA 124 DE 2001	CAMARA	Se reglamenta el Art.15 C.N., existencia y funcionamiento de los bancos de datos.(Gaceta del Congreso No.630 Dic.7/01)	Publicado el informe de ponencia para el primer debate
LEY ESTATUTARIA 201 DE 2003	CAMARA	Se regula el derecho de acceso a la información de interés público, comercial y financiero, obligaciones fiscales y parafiscales, servicios públicos domiciliarios	No se convirtió en ley por falta de trámite
LEY ESTATUTARIA 71 DE 2002	SENADO		
LEY ESTATUTARIA 74 DE 2003	CAMARA	Se regula integralmente el derecho al hábeas data y demás libertades y derechos fundamentales de las personas en bases de datos públicas y privadas	No se convirtió en ley por falta de trámite
LEY ESTATUTARIA 64 DE 2003	SENADO		
LEY ESTATUTARIA 143 DE 2003	SENADO	Protección de datos personales, se regula la recolección, tratamiento y circulación	No se convirtió en ley porque fue archivado
LEY ESTATUTARIA 071 DE 2005	CAMARA	Se dictas disposiciones generales del hábeas data y se regula información de bases de datos	
LEY ESTATUTARIA DE 2005	N/A	Protección de datos de carácter personal y se regula actividad de recolección, tratamiento y circulación de datos	
LEY ESTATUTARIA 27 DE 2006 ACUMULADO CON LEY No. 05 DE 2006	SENADO	Se dictas disposiciones generales de hábeas data, regulación de información en bases de datos financiera, crediticia y comercial de servicios	Texto aprobado por la Comisión Primera HSR
LEY ESTATUTARIA 221 DE 2007 ACUMULADO CON EL No. 05 DE 2006	CAMARA	Se dictan disposiciones generales de hábeas data y se regula en manejo de información en bases de datos personales, en especial la financiera, crediticia y comercial de servicios	Texto aprobado por la Cámara de Representantes

Tabla1. Proyectos de referencia de Protección de datos personales
Fuente: Riascos, L. (n.d.). El Habeas Data en el Derecho Público Colombiano.