LEY 1581 DE 2012: CONTEXTUALIZACIÓN DE LA NORMA A NIVEL NACIONAL E INTERNACIONAL Y ANÁLISIS DE ALGUNAS SANCIONES INTERPUESTAS.

Diana Carolina Forero Loaiza.

Santiago Velez Trucco.

Universidad Pontifica Bolivariana

Diana Carolina Forero Loaiza y Santiago Velez Trucco, estudiantes de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana en la República de Colombia, del pregrado de Derecho, analizan la ley 1581 de 2012 partiendo de una contextualización de la norma a nivel nacional e internacional para finalizar con una revisión de algunas de las sanciones interpuestas a la fecha.

Correo electrónico: dianacarolfl@gmail.com; Santupac111@hotmail.com.

RESUMEN

La presente investigación tiene como objeto el concepto de habeas data o el derecho a conocer toda información recogida o almacenada en las bases de datos lo que conlleva el acceso a las mismas donde se encuentra dicha información; además, del derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; derecho a actualizar la información; derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad. De igual manera, la aplicación el derecho al olvido, esto es, el derecho a eliminar información que se considera inútil por el transcurso del tiempo y ha perdido su utilidad.

A lo largo del texto se pretende realizar un análisis de los antecedentes históricos de la figura en las diferentes legislaciones a nivel mundial y el desarrollo legislativo nacional, especialmente teniendo en cuenta la naturaleza de ser un derecho fundamental,-otorgado por la Constitución Política de 1991.

Por último, se hará un breve análisis de las consecuencias y sanciones establecidas a nivel nacional por su violación.

Palabras clave:

Habeas Data, Libertades Individuales, Base de datos, Derecho al olvido, Derecho Positivo, Corte Constitucional, Superintendencia de Industria y Comercio.

SUMMARY

This research is aimed at the concept of habeas data or the right to know all information collected or stored in databases which entails access to them where this information is located; in addition, the right to include new data in order that a complete picture of the holder is provided; right to update information; right to information in databases is rectified or corrected in such a manner consistent with reality. Similarly, applying the right to be forgotten, that is, the right to remove information that is considered useless by the passage of time and has outlived its usefulness.

Throughout the text it is to conduct an analysis of the historical background of the figure in the different legislations worldwide and national legislative development, especially given the nature of a fundamental right granted by the Constitution of 1991.

Finally, there will be a brief analysis of the consequences and penalties established at national level for its violation.

Keywords:

Habeas Data, Individual Liberties, Database, Right to oblivion, Positive Law, Constitutional Court, Superintendence of Industry and Commerce.

INTRODUCCIÓN.

En un mundo interconectado como el que vivimos hoy, pues gracias a los avances tecnológicos, a Internet como nuevo medio de comunicación, nuestra sociedad que se ha venido transformando en una sociedad de la información y todos los cambios que se dan día a día con los avances en este nuevo ecosistema digital, han permitido la creación de nuevas empresas y el surgimiento de nuevas formas de hacer negocios**.**

Negocios que ya no sólo se dan en un plano físico sino que han traspasado incluso fronteras geográficas, haciendo uso de la tecnología. Este es un punto importante en el cual el derecho también tiene nuevos retos y nuevas áreas de impacto por regular**.**

Es por esto que hoy en día para en el contexto mundial la información es un activo inmaterial muy importante, como consecuencia de esta situación, se ha hecho necesario por parte de los diferentes Estado la búsqueda de protección a la "privacidad e integridad personal" por medio de disposiciones y normas.

En este contexto el gobierno nacional a través de la Ley Estatutaria de Habeas Data 1581 de 2012[1] pretende crear un marco legal sobre el cual sea posible la defensa integral del derecho fundamental a la intimidad, al buen nombre y todos los demás derechos constitucionales conexos.

[1] Esta Ley establece los principios generales aplicables a cualquier tipo de tratamiento de Datos Personales, incluyendo datos sensibles y datos de menores de edad, los deberes y obligaciones del Responsable y Encargado del tratamiento de la información, las consideraciones relativas a la solicitud de autorización o consentimiento de los titulares de la información y establece las reglas relacionadas con la transferencia de Datos Personales. Solamente al tratamiento de Datos Personales realizados en territorio colombiano o siempre que un Responsable o Encargado de la información que no se encuentre localizado en Colombia, se encuentre sujeto a la legislación Colombiana de conformidad con los tratados internacionales aplicables.

La Corte constitucional de Colombia lo ha definido en diferentes oportunidades como *la facultad del titular de los datos personales de exigir a las administradoras de datos el acceso, inclusión, exclusión corrección, adicción, actualización y certificación de los datos, así como la limitación en las posibilidades de su divulgación, publicación o cesión, de conformidad con los principios que regulan el proceso de administración de datos personales. Asimismo, ha señalado que este derecho tiene una naturaleza autónoma que lo diferencia de otras garantías con las que está en permanente relación, como los derechos a la intimidad y a la información*[2].

Este derecho va más allá de su consagración en la Carta Política, se trata de ~~es~~ un elemento esencial del derecho informático y de las nuevas tecnologías.

Es deber del Estado proteger el derecho de Habeas Data y garantizar su respeto por parte de a las empresas privadas y la administración. Resulta claro que los datos personales son una extensión de la personalidad del individuo y le pertenecen. En consecuencia, cualquier uso, divulgación con o sin su consentimiento por parte de un tercero debe ser de acuerdo a las exigencias sociales, con el respeto a la constitución y la ley.

En este sentido, resulta clave la custodia y el uso de esa información, en la cual las empresas deben tener un deber de cuidado en el manejo de sus bases. La ley de Habeas Data,

---

[2] **Sentencia C-748/11**. Proyecto de ley estatutaria de habeas data y protección de datos personales. Objeto. Control de constitucionalidad de los proyectos de ley estatutaria. **Sentencia C-1011/08**. Proyecto de ley estatutaria de habeas data y manejo de información contenida en bases de datos personales. Proyecto de ley estatutaria de habeas data. Devolución a la cámara de representantes por vicio subsanable/subsanación de vicio de procedimiento en la formación de la ley estatutaria de habeas data. **Sentencia T-729/02. HABEAS DATA**. Contenido y alcance**.** Principio de operatividad. **Sentencia T-176A/14**. **DERECHO AL BUEN NOMBRE Y AL HABEAS DATA.**

busca la protección de este derecho, busca garantizar que las personas que comparten sus datos con empresas que realizan negocios de comercio, puedan tener la seguridad que sus datos personales están siendo resguardados adecuadamente.

El concepto principal es que cada persona es dueña de su propia información privada. Los demás, sean personas o empresas dependen de la autorización que la persona otorgue, para usar su información con cualquier propósito, por más inofensivo que el mismo parezca.

Las implicaciones de la aplicación de esta ley 1581 de 2012 son muy significativas. Hoy el funcionamiento general de la economía depende de bases de datos que capturan información continuamente, como parte del curso diario de su actividad.

Hoy en día las empresas que tengan bases de datos personales, como administradoras de información privada de otros, deben cumplir con una serie de requerimientos legales, además, deben propender y garantizar que esta información esté completamente segura. En este sentido, su obligación es hacer el mejor esfuerzo para que no caiga en manos de extraños, limitando el uso solo para el propósito y con la intención con que fue capturada y solicitada inicialmente. Pero principalmente debe tener el consentimiento del dueño de la información para estar en la base de datos y debe tener prueba de la autorización que recibió. El no cumplimiento de esta obligación le podría acarrear fuertes sanciones, multas hasta de 2.000 SMLMV e incluso el cierre definitivo de las operaciones.

ANTECEDENTES HISTÓRICOS DE HABEAS DATA Y LA PROTECCIÓN EN LAS DIFERENTES LEGISLACIONES EN EL MUNDO.

Decir que *habeas data* es un recurso de proceso que está hecho para controlar la información que ha sido reunida en sumideros o bases de datos, el derecho lleva consigo la corrección, cancelación y la forma de establecer legalmente un límite o restricción a la circulación de estos, su definición ha sido de carácter analítico aplicada en varios países de América Latina emulando varias características del recurso de *habeas corpus*, cuyo objetivo ya conocido es de proteger la libertad individual, la función del *habeas data* es proteger la información nominativa, lo que quiere decir que resguarda la información que identifica al individuo.

El *habeas data* para el Tribunal Constitucional alemán en el año de 1983 es el *"derecho a la autodeterminación informativa*", su función era la de garantizar la capacidad que tenían las personas para tener acceso y conocer la información que de una u otra forma les interesa, que a su vez es almacenada en sumideros de datos, para su respectiva administración, lo que pudiera facilitar la tarea de eliminar o corregir datos erróneos, así como determinar sus usos (Medrano).

En los siglos XV y XVI, las cortes del King´s Beach y Common Law dieron el uso al writ para tener cierta ventaja sobre otras cortes, así como para conceder la libertad a prisioneros cautivos por el exceso en la competencia de las cortes. Writ es constituida por un acta expedida por la Corte Suprema de Justicia, por tanto los que habían ordenado la detención debían presentar el cuerpo del detenido (Bartra, 2014), en el siglo XVII, parlamentarios se apoyaron en el writ para arrestar ilegalmente por órdenes del Rey o concejo del mismo, en el año de 1640 se aprueba la ley para que las cortes del Common Law investigaran la causa verdadera de un arresto o privación de libertad.

En Suecia a partir del año 1973, se promulgó el *Data lag*, la cual creaba la norma con la cual se crea un registro público específico, el cual ordena el registro de los ficheros electrónicos de datos ya fueran de origen público o privado, a su vez también autorizaba a que dicho registro se aplicara en licencias para el manejo de datos personales y se estipuló un ente regulador y vigilante de datos personales. Para los Estados Unidos de América, en el año de 1974, a causa del escándalo Watergate y por las sospechas sobre el uso que el Gobierno pudiera hacer de los ordenadores y de los sistemas informáticos, el Congreso norteamericano promulga el Privacy Act7 (Ruiz, 2014).

Si se habla de la Unión Europea le ha dado gran prevalencia al tema de la privacidad, en muchos casos anteponiéndolo a los intereses comerciales de las empresas, con el objetivo de proteger los derechos y libertades de las personas físicas, el derecho a la intimidad y libre circulación de datos personales, derechos consagrados en las constituciones de los estados miembros (Hernandez, 2012). En los Estados Unidos ha existido mayor flexibilidad hasta el punto de la introducción de políticas propias de autorregulación de las empresas, se descargó de cierta forma en estas la responsabilidad del manejo de la información, con el objetivo de fomentar el comercio electrónico.

En Francia, ha de mencionarse la Ley N° 78-17 de 6 de enero de 1978, llamada "Ley de Informática, Ficheros y Libertades", es de vital importancia destacar que el 29 de abril de 2004, la Asamblea Nacional dispuso en segunda lectura algunas modificaciones a la ley, algunas de la reformas más significativas se ocupan del tratamiento de las infracciones, las correspondientes a la protección de datos, la biometría, los servicios secretos y las sanciones pronunciadas por la Comisión Nacional de Informática y Libertades, autoridad de aplicación de la ley (Bazán, 2005).

En México, decir respecto al derecho a la información que se incorporó a la carta magna en 1977, por medio de la reforma del artículo 6° de la Constitución Política de los Estados Unidos Mexicanos, sin embargo a partir del año 1948, la Declaración Universal de Derechos Humanos de las Naciones Unidas, en el artículo 19 menciona el derecho a poder investigar y ser receptor de información, también la posibilidad de difundirla por cualquier medio, muy anterior a la aprobación de la Declaración Universal de Derechos del Hombre, el 10 de diciembre de 1948, se celebró la Conferencia de la Organización de las Naciones Unidas sobre la libertad de información, el derecho emana de una prolongación de la libertad de pensamiento, una base esencial del modelo democrático (Instituto de Transparencia e Información Pública de Jalisco , 2010) . En México, cada Estado tiene la responsabilidad de establecer los modos que garanticen la transparencia en los entes públicos, así como el derecho de los ciudadanos para acceder a la información pública, desde la perspectiva de que toda la información que esté en poder de los entes públicos es de acceso precisamente público.

A la vanguardia de los países americanos en establecer constitucionalmente normatividad específicas fue Guatemala, que en la Constitución de 1985, estableció "art. 31. Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos".

En cuanto a Brasil en el año de 1988 estableció únicamente un derecho de control sobre los datos de carácter personal y de reglamentar que la informática no debe afectar a la intimidad de las personas pero sin llegar a establecer los principios relativos al tratamiento de los datos ni reconocer expresamente el derecho al control de ellos, reconoció por primera vez una garantía

específica del derecho a la protección de los datos, bautizándola “hábeas data”, en clara simetría con la acción de hábeas corpus como se observará sólo a estas dos acciones se las reconoce como “gratuitas” (Puccinelli, 2004).

Es valida retomar la idea o el concepto que se viene desarrollando en los últimos tiempos, se trata de la autodeterminación informativa. Dice Lidia Viggiola y Eduardo Molina Quiroga, de la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente los almacenados mediante medios informáticos (Solimano, 2011). Aclaran luego los autores que es un derecho personalísimo, y que ha logrado autonomía con relación a otros derechos fundamentales, entre los que se encuentran tradicionalmente el derecho a la intimidad o privacidad.

En España el derecho a la intimidad viene recogido en el artículo 18 de la Constitución, que acoge un contenido amplio de intimidad (Cuadrada, 2007). Junto a la declaración general de positivización del derecho, se reconocen específicamente algunas facetas del mismo como la intimidad domiciliaria, la libertad y confidencialidad de las comunicaciones privadas o el secreto de las comunicaciones, para acabar con la constitucionalización del habeas data o faceta informática de la intimidad.

Es el caso, entre otros, de Perú que desde la perspectiva de su habeas data incluye el derecho de acceso a la información pública y el derecho de rectificación o respuesta. En Paraguay también comprende, además de los consabidos derechos personales como privacidad, no discriminación, reserva sobre convicciones políticas o religiosas, otros derechos personales de índole patrimonial, referidos a información sobre bienes o datos sobre bienes.

La protección de los datos personales está en el artículo 33 de la Constitución de Argentina: *"Las declaraciones, derechos y garantías que enumera la Constitución, no serán entendidos como negación de otros derechos y garantías no enumerados; pero que nacen del principio de soberanía del pueblo y de la forma republicana de gobierno"*. En Argentina la Ley 25.326 estipula los principios regentes sobre la protección de los derechos, los derechos de los titulares de los datos, define la información sensible, establece los usuarios y responsables de archivos, registros y bancos de datos, calidad de datos, órganos de control; sanciones administrativas y penales, y determina la acción de protección de los datos personales o sea la acción de hábeas data (BANCO INTERAMERICANO DE DESARROLLO, 2005).

DESARROLLO DE LA LEY HABEAS DATA NORMA A NIVEL NACIONAL.

El derecho fundamental al habeas data tiene la consagración constitucional por medio del artículo 15 de la constitución Política de 1991 y el progreso jurisprudencial a partir del año 1992, por parte de la Corte Constitucional, en donde se han desarrollado los derechos de los ciudadanos a tener conocimiento de la composición, actualización y rectificación de las informaciones que se hubieren acumulado sobre ellas en los bancos de datos o archivos, y los demás derechos, libertades y garantías constitucionales (UGC, 2015).

La información es parte fundamental en el mundo de telecomunicaciones actual, es por esa razón el 17 de octubre de 2012 el Gobierno Nacional promulgo la Ley Estatutaria 1581 de 2012, se habla de esta como ley estatutaria toda vez que se entiende que la misma está principalmente instituida para la regulación y protección de los derechos de los titulares, la misma conto con un trámite especial pues para su expedición se aprobó por mayoría absoluta en

las cámaras; la misma fue expedida exclusivamente por el Congreso durante una misma legislatura; fue revisadas por la Corte Constitucional Mediante la Sentencia C-1011-08 de 16 de octubre de 2008, en la cual se efectuó la revisión de constitucionalidad del Proyecto de Ley Estatutaria No. 27/06 Senado – 221/07 Cámara (Acum. 05/06 Senado) "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.", para ejercer sobre esta un control previo de constitucionalidad mediante la Sentencia de la Corte Constitucional C – 748 de 2011. Por medio de esta ley se dictan disposiciones generales en referencia de la salvaguarda de datos personales, el objetivo de dicha ley es regular el derecho fundamental de hábeas data y señalar el grado de importancia en el procedimiento del mismo. Dicha ley propende por la protección de los datos personales registrados en cualquier sumidero o banco de datos que permite realizar acciones, semejantes a la recolección, almacenamiento, uso, circulación o eliminación, lo cual hace referencia al tratamiento que las entidades de talante público o privada, es decir que la Ley Estatutaria o ley de especial de jerarquías, tiene el objetivo primordial proteger los derechos y deberes primordiales, de igual manera los procedimientos y recursos para su protección, también mencionar que la Jurisprudencia Constitucional ha tratado desde el principio el derecho al hábeas data como una garantía del derecho a la intimidad, conforme a esa idea se hablaba de la salvaguarda de los datos que sean del dominio de la vida privada y familiar, comprendida como el entorno individual impenetrable en donde se puede realizar su proyecto de vida y en donde ni el Estado u otros actores particulares pueden intervenir (Certicámara, 2013).

Es significativo subrayar que el derecho al habeas data involucra a su interior varios derechos, como lo son la intimidad y el buen nombre. Siendo importante destacar que los

derechos a la intimidad y al *Habeas Data* son instituciones jurídicas, que aun siendo independientes, se enlazan y perfeccionan entre sí (Mejía, 2008). La intimidad envuelve la posibilidad de reclamar respeto por parte de los demás en relación con el ámbito que le interesa solo al individuo y, que se refleja en la protección de las posesiones privadas, de los gustos particulares y de las actitudes personalísimas (Sentencia T–522, 1997). Este derecho se asocia con el concepto de lo privado, lo que lo restringe a la órbita de lo familiar y de lo personal.

La Corte Constitucional ha manifestado que "no vacila en reconocer que la prevalencia del derecho a la intimidad sobre el derecho a la información, pues si bien el mismo implica la posibilidad de recibir, buscar, investigar, almacenar, procesar, sistematizar, analizar, clasificar y difundir informaciones, concepto éste genérico que cubre tanto las noticias de interés para la totalidad del conglomerado de cualquier índole y los datos almacenados y procesados por archivos y centrales informáticas. El mismo no es absoluto ni puede alegarse la garantía de su pleno disfrute como argumento para desconocer derechos de los asociados ni para evadir los necesarios controles estatales sobre la observancia del orden jurídico o sobre la prestación de los servicios que permitan canalizar informaciones al público. Es la consecuencia necesaria de la consagración de la dignidad humana como principio fundamental y valor esencial, a la vez, del Estado social de derecho en que se ha transformado hoy Colombia, por virtud de lo dispuesto en el artículo primero de la Carta de 1991. En efecto, la intimidad es, como lo hemos señalado, elemento esencial de la personalidad y como tal tiene una conexión inescindible con la dignidad humana. En consecuencia, ontológicamente es parte esencial del ser humano. Sólo puede ser objeto de limitaciones en guarda de un verdadero interés general que responda a los presupuestos establecidos, por el artículo 1a de la Constitución. No basta, pues, con la simple y genérica

proclamación de su necesidad: es necesario que ella responda a los principios y valores fundamentales de la nueva Constitución" (Barón Angarita, 1992) .

Por otra parte el derecho al buen nombre, ha sido definido por la Corte Constitucional como la reputación que acerca de una persona tienen los demás miembros de la sociedad en el medio en el cual éste se desenvuelve. El buen nombre es un derecho que presume la constante valoración a través del tiempo de la conducta del individuo, es una valoración individual y colectiva que tiene su origen en todos los actos y hechos que una persona realice, por medio de los cuales la comunidad realiza un juicio de valor sobre su comportamiento. No se refiere únicamente al concepto que se tenga de una persona, sino también a la "buena imagen" que esta genera ante la sociedad. El cual se relaciona con el derecho a Habeas data toda vez que el mismo se viola cuando sin ni causa cierta y real, se propagan en forma o directa o personal, informaciones falsas o erróneas o especies que distorsionan el concepto público que se tiene del individuo y que, por lo tanto, tienden a socavar el prestigio y la confianza de los que disfruta en el entorno social en cuyo medio actúa, o cuando en cualquier forma se manipula la opinión general para desfigurar su imagen. Por lo anterior se puede establecer que "*la protección del derecho al buen nombre se circunscribe a que la información contenida en base de datos sea información sea cierta y veraz, esto es, que los datos contenidos en ella no sean falsos ni erróneos* (T-658, 2011).

Un problema jurídico posterior planteado por la Corte Constitucional es cuando se vuelve más exigente y sensible el derecho al Hábeas Data en el momento que se ven vulnerados por derechos a la honra y al buen nombre. En ese caso la Corte Constitucional señaló que *"Conforme a estos principios toda persona tiene derecho a que lo que se exprese, sienta y piense de él por los demás corresponda a una estricta realidad de sus conductas y condiciones personales,*

especialmente de sus bondades y virtudes, de manera que la imagen no sufra detrimento por informaciones falsas, malintencionadas o inoportunas […]*por supuesto, es más exigente y estricto cuando se trata de relaciones o situaciones públicas, dado el carácter del derecho que se protege, el cual se desenvuelve muy especialmente ante una opinión circundante más o menos amplia y comprensiva de una gran variedad de relaciones personales*" (Greiffenstein, 1992).

En Colombia el Habeas Data es una garantía y un derecho fundamental dado que "pretende la protección de situaciones y condiciones indispensables para que las personas puedan desarrollar sus proyectos vitales sin obstáculos y con decoro en el contexto de la sociedad de la información" (Mejía, 2008).

Han sido muchos y complejos los problemas jurídicos se ha planteado la Corte en cada una de las sentencias emitidas con el objetivo de dar respuesta a los casos y a conciliar los derechos fundamentales en tensión (Rojas, 2013). Una de los primeros interrogantes jurídicos planteados por la Corte Constitucional es si la acción de tutela es aplicable para la protección del Hábeas Data, entonces se contempla el alcance de la ley cuando esta hace referencia de lleno a que es procedente cuando no existe otro herramienta de protección. En ese sentido dice la Corte Constitucional que "Es claro entonces que el otro medio de defensa judicial a que alude el artículo 86 debe poseer necesariamente, cuando menos, la misma eficacia en materia de protección inmediata de derechos constitucionales fundamentales que, por su naturaleza, tiene la acción de tutela. De no ser así, se estaría haciendo simplemente una burda y mecánica exégesis de la norma, en abierta contradicción con los principios vigentes en materia de efectividad de los derechos y con desconocimiento absoluto del querer expreso del Constituyente" (Barón Angarita, 1992).

Es claro que ahora el hábeas data es esencialmente un derecho autónomo, que está conformado por la independencia informática y la libertad económica.-Este derecho, necesita para su autonomía de la protección real de una serie de elementos que lo aseguren, dichos elementos no sólo pueden depender de la actividad de los jueces, sino además han de estar encuadrados en una institucionalidad administrativa que aparte de ejercer control y vigilancia tanto para los sujetos de derecho público como privado (FNG, 2014) ratifiquen el cumplimiento efectivo de la protección de datos.

Por otra parte, por la naturaleza de su carácter técnico, el Estado ha de tener la capacidad de marcar políticas públicas en la materia, careciendo de cualquier interferencia de carácter político para la realización de esas decisiones.

En sus alcances mínimos que emanan del derecho de hábeas data está la facultad que tienen las personas a tener acceso a la información que sobre ellas están contenidas en bases de datos, aquello implica el conocer los datos contenidos en las mismas, adicionalmente, el derecho a introducir nuevos datos con motivo de que se provea una imagen completa del interesado y el derecho de poder hacer actualizaciones a la información (HCHR, 2003), en otras palabras, a que la información que se encuentre en bancos de datos sea rectificada o corregida, de manera que se ajuste a la realidad, o la posibilidad a eliminar información de un banco de datos, ya sea porque se hiso un uso indebido de ella, o por voluntad del interesado exceptuando las previstas en la norma.

El tratamiento y flujo de los datos personales debe garantizar la protección de los derechos fundamentales de sus titulares ante los posibles atropellos que sean objeto por acción de los administradores de bases de datos o archivos, teniendo acceso a información falsa,

inexacta, incompleta o sin autorización por parte del titular. En respuesta a esta preocupación, fueron promulgadas las leyes 1266 de 2008 y 1581 de 2012, la primera se ocupa del tratamiento de la información que se encuentra en bases de datos personales de carácter financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Posteriormente la segunda, hace, referencia a mandatos generales para la protección de datos personales. Con el tiempo y el desarrollo jurisprudencial se ha conseguido establecer un marco normativo para una protección real de los titulares de la información, manejada por los usuarios, operadores o fuentes de información.

Para la Corte Constitucional y la normatividad ya mencionada se ha dicho reiteradamente con el fin de proteger los derechos del titular de la información, manifestando que los datos personales han de ser manejados con el consentimiento previo y expresa del ciudadano, además no se puede suministrar información desactualizada, falsa y no autorizada (CONTRERAS, 2014).

La manera exagerada como se administra el derecho al Habeas Data podría verse como un obstáculo comercial no solo en la transferencia y autorización de datos personales de los ciudadanos, también para las empresas que tienen las bases de datos, toda vez que las mismas deberán implementar mecanismos que permitan dar cumplimiento a esta normatividad, principalmente en la búsqueda de las autorizaciones de los titulares, generando en esta la carga más relevante que se les ha impuesto a los comerciantes y empresarios, pues obtenerla dificulta más sus prácticas comerciales e implica unos costos tanto económicos como de oportunidad, en los que antes de la vigencia de la ley 1581 de 2013, no tenían que incurrir, generando en ellas la necesidad de crear una cultura diligente de cumplimiento en cuanto a la privacidad y correcta administración de las bases de datos conformadas por Datos Personales, creando así una

conciencia en el ámbito profesional y desarrollo normal de los negocios, en cuanto a la necesidad de usar correctamente Datos Personales en cumplimiento a la norma vigente en la materia. Pero también es importante resaltar que si bien el cumplimiento de la del derecho de Habeas Data conlleva unos cambios en el sector comercio en cuanto a lo que refiere al dar complimiento de la misma es una clara manifestación del compromiso que adquirió el país en la protección de este derecho, lo cual permitirá eliminar la barreras en la transferencia de datos personales a Colombia, ya que antes de entrada en vigencia de la ley 1581 Colombia era considerado como un país no seguro en protección de datos por la Unión Europea, pero con la Ley 1581 de 2012 se pretende que Colombia sea un mercado más atractivo en la región para lo que se relaciona con tercerización de servicios, logrando con esto un impulso importante en el sector empresarial, generando así más empleo y levantando los obstáculos comerciales que se tenían en cuanto a la transferencia de datos personales de ciudadanos europeos para que sean tratados en Colombia.

Resulta importante establecer que la constitución política de 1991 consagro los derechos a la libertad económica e iniciativa privada, de los más mencionados se recuerda la libertad de empresa, establecidos en el artículo 333:

> "*La actividad económica y la iniciativa privada son libres dentro de los límites del bien común. Para su ejercicio nadie podrá exigir permisos previos ni requisitos, sin autorización de la ley. La libre competencia económica es un derecho de todos que supone responsabilidades. La empresa, como base del desarrollo, tiene una función social que implica obligaciones. El estado fortalecerá las organizaciones solidarias y estimulara el desarrollo empresarial.*

> *El estado, por mandato de la ley, impedirá que se obstruya o restrinja la libertad económica y evitará o contralará cualquier abuso que personas o empresas hagan de su posición dominante en el mercado nacional. La ley delimitara el alcance de la libertad económica cuando así lo exijan el interés social, el ambiente y el patrimonio cultural de la nación."* (Constitución Política de Colombia, 1997)

Siendo con esto claro que si bien como se establece en la Sentencia C–263 de 2011, la libertad de la autonomía de la voluntad privada del sector empresarial, la cual no es más que la facultad que tiene toda persona de realizar actividades de carácter económico según sus preferencias o habilidades, con miras a crear, mantener o incrementar su patrimonio, cuya iniciativa es ciertamente libre, dichas libertades no son absolutas y pueden ser limitadas por el Estado.

Conforme a lo anterior, hoy en día, uno de los límites más característicos en el mundo empresarial y comercial es el derecho fundamental del Habeas Data, que si bien, como se mencionó, apareció en Colombia con la promulgación de la Constitución Política de 1991, fue hasta el año 2013 en el cual entro en vigencia la ley 1581 de 2012 y su decreto reglamentario 1377 de 2013, los cuales se convirtieron en un efectivo limitante para la libertad de empresa e iniciativa privad, pues es con la misma se imponen deberes concretos a todos aquellos que pretendan utilizar los datos de las personas y si no se cumple con dichos deberes no se podrá realizar tratamiento sobre la información. Generando confusión y muchas preguntas para los comerciantes que ya se encontraban familiarizados con la práctica de ciertos hábitos en el uso de los datos personales de sus usuarios, las cuales, teniendo en cuenta las citadas normas, ya no podían realizar más.

Puesto que el sector empresarial y para el mundo comercial, la mayor importancia se la llevan los consumidores, y por lo tanto sus datos personales, y el tratamiento sobre los mismos, son de gran utilidad para que el comerciante o empresario logre capturar un mayor número de consumidores a través de estrategias de mercadeo y de esta forma obtener el beneficio o ganancia buscado. De acuerdo a esto, las obligaciones que la ley 1581 de 2013 impuso a todos aquellos que quisieran darle un tratamiento a los datos de las personas, en este caso de los consumidores, género que los empresarios o comerciantes tuvieran que replantear la forma de desarrollar sus actividades, pues estaban acostumbrados a vender bases de datos, capturar las mismas sin ningún tipo de consentimiento del titular y muchas veces no respetando en muchos casos, el derecho fundamental del Habeas Data. Generando también unos costos económicos, puesto que deben realizar la implementación de formularios, capacitaciones, publicidad, herramientas tecnológicas, entre otros. Y los costos de oportunidad, loa cuales se podrían entender como los beneficios o ganancias que los empresarios y comerciantes dejan de percibir por no poder usar libremente los datos, en los casos en que no cuenten con la autorización expresa para determinada finalidad.

Ya que como lo establece la Corte Constitucional en la Sentencia C–748 de 2011, se prohíbe a todas las entidades, públicas o privadas, realizar un tratamiento sobre los datos personales sin previo consentimiento del titular de esta información. Entendiéndose como tratamiento “cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión” (Artículo 3, Ley 1581 de 2012). Es decir cualquier operación que se pretenda hacer con el dato personal, con o sin ayuda informática, que a diferencia de otras legislaciones, en la nuestra no se circunscribe únicamente a

procedimientos automatizados, por lo tanto aquí se protegen los datos que reposen en bases de datos tanto manuales, como las que se apoyan en las nuevas tecnologías.

El legislador tuvo en cuenta todas estas dificultades que podría generar la implementación de dicha la ley 1581 de 2012, y por esta razón otorgó un periodo de transición, el cual radicó en que las personas que a la fecha de la entrada en vigencia de la ley ejercieran alguna de las actividades allí reguladas tendrían un plazo de hasta seis (6) meses para adecuarse a las disposiciones contempladas en esta ley (Artículo 28, ley 1581 de 2012.) . Sin embargo una vez venció este plazo, en abril del año 2013, los empresarios y comerciantes que realizaban actividades con bases de datos personales, presentaron varios inconvenientes entre ellos la dificultad de conseguir en seis meses la autorización de cientos, o miles de consumidores almacenados en sus bases de datos o archivos. Y el dejar de utilizar estos datos, pues implicaba una gran desventaja para su actividad económica, y en virtud de la ley 1581 de 2012, ya no se podían seguir desarrollando las actividades con el uso de los datos personales, sin la autorización expresa para ello. Por lo tanto, se hizo necesario expedir el decreto 1377 de 2013, por medio del cual se reglamentó parcialmente la ley 1581 de 2012, que simplificó ampliamente el modo de cumplir con esta normatividad, pues permitió que la autorización de los datos recolectados antes de la expedición de esa norma, se consiguiera a través de mecanismos alternos tales como diarios de amplia circulación nacional, diarios locales o revistas, páginas de internet del responsable, carteles informativos, corres electrónicos entre otros (Numeral 3, artículo 10. Decreto 1377 de 2013). Estos mecanismos radicaban en dar a conocer a los consumidores en general, y en algunos casos en particular, la existencia de un tratamiento de datos personales dentro de determinada empresa, las finalidades de dicho tratamiento y los derechos que las personas tenían como titulares de esta información; así, si dentro de los 30 días hábiles siguientes a la

implementación de uno de los mecanismos de comunicación anteriormente mencionados, los titulares de la información no manifestaban al responsable su intención de que se suprimieran sus datos del tratamiento del cual se les estaba dando conocimiento, la ley autorizó a los responsables o encargados del tratamiento para continuar con el manejo del mismo. (Numeral 4, artículo 10. Decreto 1377 de 2013)

Por otra parte es importante resaltar que la ley 1581 de 2012 desarrollo unos principios los cuales versan sobre protección de datos personales de carácter general, pero antes de ahondar en los mismos, es oportuno aclarar que la ley 1266 de 2008 ya había desarrollado principios tales como Principio de veracidad, Principio de finalidad, Principio de circulación restringida, Principio de interpretación integral de derechos constitucionales, Principio de seguridad, Principio de temporalidad de la información, y Principio de confidencialidad los mismos solo hacían alusión para el manejo de la información contenida en bases de datos personales financieros, crediticios, comerciales y/o de servicios, los cuales si bien podrían ser similares, con la nueva regulación se extendió el ámbito de aplicación. De acuerdo con lo anterior, se hará referencia solamente a los principios delineados por la ley 1581 de 2012, en su artículo 4, los cuales son los siguientes:

> **Principio de legalidad**. Se refiere al tratamiento de los datos como una actividad reglada, que debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen.
>
> **Principio de finalidad.** Señala que las actividades de recolección de datos personales obedecen a una finalidad legítima de acuerdo con la

Constitución y la ley; y determina que la finalidad para la cual será usada dicha información, deberá comunicarse al titular, de manera previa o concomitante con el otorgamiento de la autorización por parte del mismo, cuando ella sea necesaria o, en general, siempre que el titular solicite información al respecto.

Principio de libertad. Según el cual el tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Principio de veracidad o calidad. Mediante el cual la información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible, prohibiendo el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de transparencia. Por medio del cual se debe garantizar el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento de la información, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Principio de acceso y circulación restringida. Por medio del cual se busca establecer que la administración de los datos personales se sujete a los límites que se derivan de su naturaleza, de la norma estatutaria y de los principios que le son aplicables a esta actividad, en especial los de temporalidad de la información y finalidad del banco de datos. Así mismo, en virtud de este principio los datos personales, salvo 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 a los usuarios autorizados para ello, en los términos de la disposición estatutaria.

Principio de seguridad. Se refiere a que en la información personal contenida en bases de datos y la resultante de las consultas que realicen los usuarios, se incorporen las medidas técnicas necesarias para garantizar la seguridad de los registros, a fin de evitar su adulteración, pérdida, consulta o uso no autorizado.

Principio de confidencialidad. Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores

que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley.

Con lo anterior, se pretende hacer una pequeña semblanza del derecho de Habeas Data, referenciando brevemente los antecedentes en Colombia, la realización de un análisis de la situación actual en la que está el mencionado derecho, identificando los elementos fundamentales del dato personal y del dato sensible, los principios vigentes y la posición adoptada por la Corte Constitucional referente a este derecho.

MECANISMOS DE VIGILANCIA Y SANCIÓN.

El derecho de Habeas Data ha violado cuando la información contenida en el archivo o base de datos es recogida de manera ilegal, sin el consentimiento del titular del dato, o esta es errónea o recae sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente.

Con la promulgación de la ley 1581 se creó la Autoridad de Protección de Datos Personales de la Superintendencia de Industria y Comercio, con miras de que dicha entidad ejerciera la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

Tiene como principales Funciones velar por el cumplimiento de la legislación en materia de protección de datos personales; Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo

el derecho de hábeas data. Para ~~el~~ tal efecto, siempre que se desconozca el derecho, podrá disponer el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos; Disponer el bloqueo temporal de los datos cuando, de la solicitud y ~~de~~ las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva; Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos; Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento.

De acuerdo con el artículo 23 Ley Estatutaria 1581 se consagran las Sanciones que podrá interponer La Superintendencia de Industria y Comercio a los Responsables del Tratamiento y Encargados del Tratamiento las cuales van desde multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes las cuales podrán ser sucesivas mientras subsista el incumplimiento que las originó. También se podrán suspender de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. Pasando por el Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión y no se hubieren adoptado los correctivos ordenados, hasta el cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

ANÁLISIS DE ALGUNAS SANCIONES.

SENTENCIA DE LA CORTE CONSTITUCIONAL T-058 DEL AÑO 2013, que el caso tiene como elemento la posible violación al *habeas data*, de parte de una Universidad a un

ciudadano que fuere estudiante suyo. La correspondiente sentencia nos muestra uno de los tantos panoramas que se pueden configurar cuando se involucra el habeas data, su protección es trascendental y como en este caso en específico, puede llegar a manejar una conexidad directa con otros derechos sumamente relevantes como lo son el de la educación, así pues, es posible determinar que un mal manejo de la información personal de las personas, puede terminar vulnerando un sin número de esferas que deben primar aun ante la publicidad de datos verídicos con aras de no limitar el satisfactorio desarrollo al que tiene derecho todo ciudadano.

En el respectivo caso, el apoderado de la universidad buscaba que se determinara la existencia de temeridad con la presentación de la nueva acción de tutela, alegando que tanto los hechos y pretensiones como los fundamentos expuestos, coincidían con la primera acción de tutela del estudiante, la cual ya había sido decidida en su contra, y por lo tanto insistía que no había lugar a tramitar la nueva tutela.

ACCION DE TUTELA TEMERARIA**,** a pesar de que se encuentran grandes similitudes entre las dos acciones de tutela, se termina configurando su inexistencia. La interposición de la nueva acción de tutela estaba nutrida de nuevos sucesos de gran relevancia, los cuales tenían que ver con certificaciones de estudio que podían ser determinantes para concluirse la vulneración al habeas data y por consiguiente al buen nombre y sobre todo para la relevancia de la actora, su derecho a la educación, el cual a razón de los nuevos certificados a los que se aludía, se estaba obstaculizando. A su vez, las nuevas pretensiones se enfocaban en lograr que la universidad omitiera todo dato negativo relacionado con sanciones disciplinarias de las mencionadas certificaciones. Por último, con base en lo anterior, la nueva acción de tutela lograba constituir nuevos fundamentos legales y constitucionales sobre la vulneración a los derechos alegados.

De conformidad con lo anterior y según los requisitos necesarios para que se configure la temeridad con base en la jurisprudencia, se descarta su presencia y se determina que los nuevos hechos que dificultan la continuidad del desarrollo académico del estudiante, se prestan para hacer procedente la nueva acción de tutela con miras a la protección de los derechos involucrados.

El magistrado Alexei Julio Estrada dice que el habeas data es un derecho de doble naturaleza. Por una parte, goza del reconocimiento constitucional de derecho autónomo, consagrado en el artículo 15 de la Constitución y, por otra, ha sido considerado como una garantía de otros derechos en la medida en que los protege mediante la vigilancia y cumplimiento de las reglas y principios de la administración de datos, por ejemplo el habeas data opera como garantía del buen nombre cuando se emplea para rectificar el tratamiento de información falsa, opera como garantía a la seguridad social, cuando se emplea para incluir , en la base de datos, información personal necesaria para la prestación de los servicios de salud y prestaciones propias de la seguridad social, opera como garantía del derecho de locomoción , cuando se solicita para actualizar información relacionada con la vigencia de ordenes de captura, cuando estas por ejemplo han sido revocadas por la autoridad competente. Como derecho autónomo, tiene el habeas data un objeto protegido concreto: el poder de control , consistente en la facultad que se lo otorga al titular de los datos personales, ya sea persona natural o jurídica, de poder demandar de sus administradores, ósea todos aquellos que hacen de receptores y sobre los cuales recaen, el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de aquella información, así como de dar cumplimiento al principio de restricción de circulación, el cual hace referencia a que a menos de que la información sea pública, los datos personales no

podrán ser accesibles por internet o por otros medios de divulgación o comunicación masiva, salvo que dicho acceso sea técnicamente controlable para brindar un conocimiento restringido solo a sus titulares o personas autorizadas. El poder de control permite a su titular, exigir todas aquellas conductas de conformidad con los demás principios que regulan el manejo de datos personales y los cuales tiene fines constitucionales.

DERECHO A LA EDUCACION Y HABEAS DATA-Vulneración por universidad al expedir certificado de estudios que registra sanciones disciplinarias por plagio sin consentimiento previo, expreso e informado de la estudiante.

La Universidad expidió unas "certificaciones de estudio" con un contenido totalmente diferente al que corresponde a una certificación de este tipo y profirió un documento que contiene información sobre su órbita personal sin su consentimiento previo, expreso e informado y que, de manera desproporcionada, ha interferido claramente en su derecho al habeas data y de contera a la educación. Esta última vulneración se concreta en la negativa de la Universidad CC de admitir a la peticionaria en el programa de Finanzas, Gobierno y Relaciones Internacionales, luego de haber recibido las mencionadas "certificaciones de estudio" a pesar de que la accionante acreditó mediante los certificados de notas, su excelencia académica. Encuentra la Sala que la Universidad, al proferir las certificaciones, interfirió de manera desproporcionada en los derechos al habeas data y a la educación de la actora en la medida en que: (i) la Universidad no evidenció fines específicos para divulgar el dato, (ii) en consecuencia fue ilegítima la medida de divulgar el dato en si misma, (iii) por ello resultó desproporcionada y afectó no sólo el derecho al

habeas data sino una consecuente afectación al derecho a la educación, y (iv) no requirió del titular de la información su consentimiento para divulgarla.

TRATAMIENTO DE DATOS PERSONALES-Ley 1581 de 2012 le dio competencia a la Superintendencia de Industria y Comercio para ejercer vigilancia y control para garantizar los datos personales.

DERECHO A LA EDUCACION Y AL HABEAS DATA-Orden a Universidad expida certificación de estudios la cual no podrá contener elementos que permitan a un tercero inferir que estuvo procesada y sancionada disciplinariamente por plagio.

El Juzgado Tercero Penal Municipal con Función de Conocimiento de Bogotá, mediante sentencia proferida el 3 de julio de 2012 hizo un recuento de los hechos, analizó la jurisprudencia relacionada con el derecho a la educación, el principio de autonomía universitaria, el derecho al buen nombre y al habeas data y declaró improcedente la tutela.

En cuanto a las certificaciones expedidas por la Universidad BB, el Juzgado consideró que la información allí contenida corresponde al resultado de los procesos disciplinarios adelantados en contra de la actora, es decir la información se ajusta a la realidad y es "*producto de los actos y conductas de la accionante dentro de la esfera académica e institucional cuando era estudiante, de tal manera que la repercusión social que recae sobre su honra, buen nombre o en torno a su imagen que se pueda ver afectada, solo son consecuencia de su proceder, bajo su única responsabilidad, sin que sea el resultado ilegítimo del actuar de la institución académica.*"

Mediante escrito presentado ante el juez de conocimiento, la peticionaria interpuso recurso de impugnación contra el fallo proferido.

El Juzgado Veintidós Penal del Circuito con Función de Conocimiento de Bogotá, en sentencia dictada el 10 de agosto de 2012, determinó que la Universidad accionada no había incurrido en la violación al derecho a la educación, toda vez que la decisión de expulsarla de la institución educativa era el resultado del comportamiento inadecuado de la alumna y que dicha decisión había surgido después de un trámite disciplinario que se adelantó con las garantías propias del debido proceso y del derecho de defensa.

En cuanto a las certificaciones expedidas, reprochó que la accionante no hubiera acreditado haber requerido a la Universidad la modificación o actualización de sus datos, "*por lo cual, de conformidad con la jurisprudencia atrás señalada la tutela impugnada deviene confirmación."*

En este caso concreto la certificación de un dato negativo no autorizada por su titular ha afectado la posibilidad de la accionante de continuar sus estudios universitarios. En efecto, la Constitución de los derechos fundamentales debe verse *como un todo*, con partes interdependientes e indivisibles. La afectación de una de sus partes no es sólo la afectación de una parte, porque ese ataque acarrea, sin duda alguna y muy a menudo, la afectación de muchas, si no de todas las otras. Por lo tanto, un imperativo de transparencia en la argumentación demanda de parte del operador judicial identificar todos los derechos afectados por una determinada actuación u omisión de autoridades públicas (Estrada, 2013).

En relación a lo anterior, el Magistrado Luis Ernesto Vargas Silva expone el siguiente salvamento parcial de voto: Como lo expuse a la posición mayoritaria considero que el caso debió abordarse desde otra perspectiva, relacionada con el contenido de los certificados expedidos por las universidades y la vigencia de los datos negativos que pueden ser registrados

en ellos. En particular, la posibilidad de incluir la sanción disciplinaria de la estudiante en un certificado de estudios. De una parte, porque los certificados de estudios parece ser la forma oficial en que las universidades reportan el comportamiento de sus estudiantes, y de otra, para definir si pueden contener información distinta a la académica, sobre todo tratándose de un dato negativo como una sanción disciplinaria pues es cuestionable constitucionalmente si debe permanecer de forma indefinida en el reporte académico. Lo anterior hubiera permitido a la Sala pronunciarse sobre si el hecho de que se suministre el dato negativo por parte de la Universidad constituye una doble sanción o una sanción permanente que afectó el derecho al buen nombre de la estudiante en vulneración de su derecho, por ejemplo, a la educación superior.

En ese contexto, la sentencia expone que la certificación de un dato negativo no autorizado por su titular ha afectado su posibilidad de estudiar de nuevo. Sin embargo, no se evalúa el consentimiento otorgado por la accionante como parte del contrato educativo ni el reglamento de la Universidad. En efecto, la relación académica, administrativa y disciplinaria, entre la Universidad y sus estudiantes está regida por esos instrumentos sin que se haga referencia a los mismos en la providencia. Esa verificación hubiera permitido a la Sala establecer si existe consentimiento por parte del alumno y los términos en que fue otorgado a la Universidad para el manejo de la información y la administración de datos de sus estudiantes.

Al respecto, considero que el proyecto debió identificar la naturaleza de los certificados académicos pues en términos generales son el documento a través del cual las universidades reportan la conducta de sus estudiantes. Y la evidencia fáctica advierte que no funcionan de forma separada, es decir, no se expide una certificación para los antecedentes disciplinarios del alumno, otra para reportar incidentes administrativos y otra para certificar el ámbito académico.

Por otra parte, la sentencia debió profundizar el alcance de la autonomía universitaria puesto que hace referencia a la misma en los siguientes términos: "*Esta Corporación difiere de la interpretación de la Universidad BB de la autonomía universitaria ampliamente definida en la jurisprudencia de esta Corte, así como la facultad que tiene como tenedor y/o responsable de la información personal de los estudiantes de expedir certificaciones en las que divulgue información personal o datos que afecten gravemente sus derechos fundamentales*", sin hacer alusión a sentencia alguna de la Corte o justificar por qué está en desacuerdo con el ejercicio de esa potestad por parte del plantel educativo.

Finalmente, la protección otorgada está relacionada con la vulneración del derecho a la educación de la accionante lo cual se deduce de la siguiente forma: "*Por consiguiente, divulgar al público en general de manera indiscriminada información del estudiante que el centro educativo haya conocido o conozca con ocasión de sus funciones educativas, constituye una barrera al acceso al derecho de la educación.*".

Al respecto, estimo que la Universidad no ha divulgado ninguna información al público, el certificado se expidió a solicitud de la accionante, y no se demostró que se haya negado el ingreso a otro centro educativo en razón a la certificación expedida. (Vargas Silva, 2013)

En este caso en particular, la Corte pudo constatar que la vulneración del habeas data al no permitírsela a la ex estudiante la modificación, rectificación y exclusión del dato negativo pese a haberlo solicitado trajo aparejada la vulneración del derecho a la educación de la misma. Teniendo en cuenta lo anterior, es muy razonable pensar que dicho dato negativo expresamente declarado en un certificado que se sabe, va a ser estudiado por otras universidades,

termina por jugar un papel oscuro que tacha al estudiante y como consecuencia obvia, limitara su aceptación dentro de otras entidades, por tal motivo, con el fin de permitirle continuar su formación académica, a la cual tiene derecho, no es necesario que aquella información conste en la certificación, no para hacer de cuenta que nunca ocurrió o para ocultarlo, sino para omitirlo con el propósito de enfocarse en darle nuevas oportunidades al estudiante de ejercer su derecho, es necesario ponderar y para el caso prima constitucionalmente salvaguardar el derecho a la educación.

La correcta o incorrecta administración de datos personales tiene efectos, en muchas ocasiones, en las condiciones de ejercicio de los derechos fundamentales de los sujetos concernidos por dicha información. La peticionaria acude al habeas data por cuanto sabe que la información negativa que aparece en los certificados de estudio, funge como una barrera para la continuidad de sus estudios académicos; sabe que dicha información se convierte de facto en un factor de discriminación, toda vez que no fue aceptada en la Universidad CC, sin motivo alguno, inclusive luego de presentar certificados de notas con promedios de excelencia (Estrada, 2013).

En relación con el problema jurídico planteado, la Sala de Revisión considera que la Universidad BB efectivamente vulneró los derechos al habeas data, a la educación y al buen nombre de AA al expedir certificaciones en las que informó sobre los procesos disciplinarios adelantados en su contra y sus consecuentes sanciones por plagio, por lo que habrá de revocarse el fallo judicial de segunda instancia proferido el 10 de agosto de 2012 por el Juzgado Veintidós Penal del Circuito con Función de Conocimiento de Bogotá, y en su lugar, disponer la protección tutelar deprecada por la actora, en el sentido de ordenar a la institución educativa accionada que dentro de las cuarenta y ocho (48) horas siguientes a la notificación del presente fallo, expida una nueva certificación de estudio a la tutelante, cuyo contenido se refiera únicamente a los detalles

del programa académico, las asignaturas cursadas y las calificaciones obtenidas, y no consigne elemento que le permita a un tercero inferir que estuvo procesada y sancionada disciplinariamente por plagio (Estrada, 2013).

Finalmente como conclusión de la sentencia, es posible decir que existe un gran responsabilidad por parte de quienes se encargan de manejar los datos personales de las personas, y aunque por ejemplo específicamente en el caso de las universidades, estas tienen el derecho de informar de manera veraz e imparcial, existe una limitación y aquella hace referencia a los principios sobre la administración de los datos. Lo anterior significa que siempre que se maneje o haga uso de la información personal de los estudiantes por parte de las universidades, no solo se debe tener en cuenta que aquella sea cierta, es igualmente importante tener presente que con su manipulación no se vulnere o limite ninguna de sus garantías constitucionales, la finalidad de la información debe limitarse a un objetivo legal, útil y necesario en donde sí se publica algún dato que sobra y que solo puede acarrear resultados negativos para los derechos de la persona, se debe omitir con el propósito de velar por el satisfactorio desarrollo de sus derechos, nunca debe olvidarse que incluso alguien que ha incurrido en conductas reprochables, sigue contando con la posibilidad de gozar de protección y garantías constitucionales.

SENTENCIA T-176A DEL AÑO 2014, parte de la solicitud de un ciudadano que laboró en una empresa de transporte, dicho ciudadano fue víctima de un hurto, pero la empresa emite información en la cual se le pudiese relacionar con el ilícito.

DERECHO AL BUEN NOMBRE Y HABEAS DATA-En el caso se evidencia la publicidad indiscriminada de una información que al no ser actualizada, carece de certeza, lo que constituye una clara violación al principio de veracidad.

Haciendo un análisis de la situación, cabe decir que existe una delgada línea entre lo que significa manifestar algún dato incierto o falso, y entre lo que supone declarar un dato no vigente como actual, ambas circunstancias generan resultados similares en relación a la afectación del principio de veracidad y por ende pueden afectar de igual manera a la persona, aquello demuestra lo importante que es, no solo verificar que la información con la que se cuenta es verdadera, sino además que es la vigente, la actualización de los datos hace parte esencial del buen manejo de la información.

DERECHO AL BUEN NOMBRE Y HABEAS DATA-Orden a empresa transportadora eliminar de sus bases de datos cualquier información subjetiva que dé a entender que el actor se encuentra implicado, como victimario, de un hurto de un tracto camión.

Mediante fallo del 2 de julio de 2013, el Juzgado Tercero Penal Municipal con Funciones de Conocimiento de Bucaramanga, decidió negar el amparo deprecado bajo el argumento de que:

Finalmente sostuvo el a quo que "en el caso concreto no se evidencia violación alguna a los derechos fundamentales del aquí accionante, puesto que la anotación en el Boletín preventivo sólo informa las novedades en la actividad transportadora como lo son los hurtos a la mercancía o vehículos sin que este reporte o anotación este comunicado (SIC) de alguna manera que el conductor involucrado en el incidente haya tenido un algún (SIC) tipo de participación en el mismo (…)".

El 5 de julio de 2013, el señor Robinson Blanco Parra presentó recurso de impugnación en contra de la decisión de primera instancia, argumentando que:

"(…) Transportes Humadea S.A. me tiene un reporte por hurto desde el 17 de enero de 2013, que me tiene bloqueado y no me permite laborar, aparte de que atenta contra mi buen nombre. Me presenté en la empresa Transportes Humadea S.A., el 7 de mayo de 2013 y la señorita Camila Téllez Castillo, jurídica de la empresa, me dijo que yo debía una cartera de 200 millones de pesos y que por eso no me podía quitar el reporte que aparece en COLFECAR. Desde el mes de febrero no he podido ejercer mi profesión y esto me ha perjudicado gravemente mi economía, siendo que en lo sucedido también yo fui víctima".

Mediante fallo del 5 de agosto de 2013, el Juzgado Noveno Penal del Circuito con Función de Conocimiento de Bucaramanga confirmó el fallo impugnado, tras considerar que "los documentos obrantes en el expediente corroboran la existencia del hecho reportado para registro histórico pero en manera alguna un veto a alguna persona (SIC). La empresa reporta los siniestros para actualizar la base de datos de las confederaciones ante mencionadas (SIC), pero no significa que se encuentre vetado como lo afirma el accionante, sino que simplemente se trata de un dato estadístico".

La Sala considera que si bien les asiste derecho a las entidades accionadas, como parte de un gremio específico, de recopilar información y usarla en beneficio de las actividades que emprendan como asociación, pues el derecho a informar está protegido en el artículo 20 Constitucional como una garantía de todas las personas para informar y recibir información veraz e imparcial, debe reconocerse que esa facultad se encuentra limitada fundamentalmente por "el respeto por el ejercicio legítimo de los derechos fundamentales, derivado de la obligación

que el artículo 2° de la Carta le impone a las autoridades de la República para garantizar y propender por la efectividad de todos los derechos ciudadanos" y entre estos, los derechos al habeas data.

Entonces, si bien a Transportes Humadea S.A. le asiste derecho de informar tanto a COLFECAR como a DEFENCARGA los sucesos ocurridos en la actividad transportadora, para que éstas a la vez emitieran boletines preventivos a sus afiliados, dicha garantía debió ser ejercida sin la trasgresión del principio de veracidad que asiste a la administración de datos personales.

En este orden de ideas, COLFECAR y DEFENCARGA debieron tomar las medidas pertinentes para que la información contenida en sus reportes fuera actual y conforme a la realidad, evitando con ello la afectación de los derechos del señor Blanco Parra. Para ello, se recuerda que existe un deber de responsabilidad de parte de las administradoras de las bases de datos personales que no se limita al mero manejo de los mismos, sino que debe generar todo un ambiente de confianza en la gestión u operacionalización de los datos (Pretelt, 2014). En relación a lo comentado, la publicidad de información abstracta, no vigente o carente de certidumbre, afecta claramente tanto el principio de veracidad como el de finalidad que deben cumplirse por quienes manejan los datos, lo cual se ve evidenciado en la falta de objetividad y actualización, metas que se quieren alcanzar para el acopio de información personal por parte de quienes fueron los que publicaron los datos en el caso concreto, nunca se pueden olvidar los fines constitucionales, la administración de información es un asunto más delicado de lo que parece y siempre se debe tener la mayor precaución posible en aras de asegurarse la no afectación del titular o involucrado, se deben plantear todos los posibles escenarios que pueden desprenderse de

lo que se piensa informar para poder prever que consecuencias negativas podrían ocurrir y así perfeccionar y poder pulir lo que se quiere plasmar.

La Sala advierte una grave incidencia cierta y directa entre los derechos fundamentales al *habeas data*, al trabajo y al mínimo vital del señor Robinson Blanco Parra, causada por la expedición de los mencionados boletines. Lo anterior, comoquiera que se le ha impedido seguir realizando la actividad de la que derivaba su sustento, lo que lo ha llevado a incumplir sus obligaciones crediticias con sus acreedores (Pretelt, 2014).

Entonces, en el caso concreto se evidencia la publicidad indiscriminada de una información que al no ser actualizada, carece de certeza, lo que constituye una clara violación del principio de veracidad. No obstante, también se ve que el petente no hizo uso del derecho de reclamación para solicitar a las accionadas la eliminación, corrección, actualización, aclaración o rectificación de sus datos de las bases de datos por ellas administradas, sino que acudió a la acción de tutela para solicitar el amparo de sus derechos fundamentales.

En virtud de lo anterior, se ordenará a Transportes Humadea S.A., DEFENCARGA y COLFECAR, que dentro de las cuarenta y ocho (48) horas siguientes a la notificación de esta sentencia, eliminen de sus bases de datos cualquier información subjetiva que dé a entender que el señor Robinson Blanco Parra se encuentra implicado, como victimario, del hurto del tracto camión de placas XVH 855, y de las mercancías que éste contenía, las cuales eran de propiedad de Transportes Humadea S.A., y que actualicen, con información veraz y completa los datos que administran en ellas (Pretelt, 2014).

Teniendo en cuenta las decisiones tomadas en la sentencia, queda claro que toda base administradora de datos personales, debe seguir los lineamientos de los principios atinentes a la

materia, los cuales se nutren primordialmente por la veracidad, aquello prohíbe la divulgación o manejo de datos falsos, divididos o distorsionados que se presten para dar a entender hechos que efectivamente no correspondan a la realidad en relación a la persona, en cuanto al caso en concreto objeto de la sentencia, aquellas medidas condicionan el poder evitar la generación de un perjuicio que puede ser irreparable, en cuanto al hecho de tener que cargar con la tacha de reputación por figurar como implicado en un robo, lo cual seguramente le cerrara las puertas para poder continuar desarrollando la actividad que desempeñaba en algún otro lugar, viéndose afectado así, su derecho al trabajo y limitando su mínimo vital.

RESOLUCIÓN NÚMERO 36863 DEL 30 DE MAYO DE 2014 de la Superintendencia de Industria y Comercio, gira en torno al deber que tienen todos los responsables del tratamiento de datos personales, de contar con políticas para su manejo y administración, además plantea la obligación que existe de contar con aquellas directrices en medios tanto físicos como electrónicos para que estén al alcance de sus titulares en un lenguaje claro y sencillo, salvaguardando así su derecho constitucional de conocer, actualizar y rectificar la información recopilada en las bases de datos, por lo que ocurre lo siguiente:

Que el 25 de noviembre de 2013, la señora Chris Caro se comunicó vía chat de atención al cliente de Carulla, solicitando la corrección del registro de su nombre pues estaba mal escrito y además pedía que se le suministrara copia de la política de protección de datos implementada porque quería conocer el procedimiento para el ejercicio de su derecho de habeas data (SIC, 2014).

Revisando los hechos materia de investigación resulta evidente que la señora Chris Caro el 25 de noviembre de 2013, accedió a través de la página web www.carulla.com al foro o chat de "servicio al cliente" buscando la corrección de su nombre, el cual se encontraba mal incorporado en la base de datos del programa de fidelización "Súper Clientes Carulla". De acuerdo a lo manifestado vía chat, la señora Chris Caro había solicitado la corrección del mismo hacia tres meses, sin que al 25 de noviembre de 2013 hubiese sido corregida su información personal. Dada la falta de trámite de su solicitud, la quejosa se vio avocada a entrar al chat en mención en busca de orientación sobre la manera en que debía tramitar su solicitud de corrección de información, así como verificar la política de tratamiento de datos personales, a través de cual pudiera conocer los mecanismos habilitados para tal fin (SIC, 2014).

De lo anterior se puede concluir claramente que la sociedad investigada, al tener habilitado única y exclusivamente un correo electrónico para la atención de consultas y reclamos para que los titulares ejerzan su derecho a conocer, corregir, actualizar y suprimir sus datos personales o revocar la autorización otorgada, suministró información errada, impidiéndole la atención debida de su petición y vulnerando abiertamente el derecho de habeas data de la Titula pues Almacenes Éxito S.A, le manifestó a la señora Chris Caro que debía acercarse a "un punto de servicio Carulla" para que su petición fuera atendida, canal que de conformidad con la política de tratamiento, no era el medio apto para el ejercicio del derecho fundamental.

CONCLUSIONES

1. **ORIGEN DEL HABEAS DATA:** El hábeas data surge en el contexto internacional a partir de la necesidad que se manifiesta en diferentes partes del mundo de consagrar derechos en relación con la información de las personas, sus primeros antecedentes se nutren de esfuerzos que buscan preservar esferas personales y evitar perturbaciones a la privacidad por parte de quienes tenían acceso a aquellos datos, tal y como ocurrió en Estados Unidos respecto de la información que recaudaba el Gobierno de sus ciudadanos, situación que debía tener un control. Con el tiempo, las regulaciones de la materia fueron evolucionando hasta contemplar de manera más justa la utilización de los datos inherentes a cada persona, logrando que hoy día los titulares de la información sean verdaderos propietarios y por ende gocen de facultades que les permitan una autonomía para determinar el uso que se le da a los datos que los involucran.
2. **HABEAS DATA EN COLOMBIA:** El hábeas data se origina en nuestra legislación como un derecho fundamental y un mecanismo jurídico y eficaz a la hora de salvaguardar la intimidad, el buen nombre y los demás derechos conexos frente a las nuevas tecnologías de informáticas que contemplan las bases de datos. Como resultado de actividad jurisprudencial, con el tiempo se fueron llenando vacíos sobre el tratamiento de datos, inicialmente creándose la ley 1266 de 2008 y la cual solo se enfocaba en la información financiera, hasta llegar a la ley 1581 de 2012 que maneja un carácter general y la cual aplica para todos los ámbitos de recolección de datos de las personas, discriminado de manera contundente y completa la nueva era del uso de información, en ella se especifican entre otros, deberes que tienen los destinatarios de la información y las consecuencias que recaerán sobre ellos en los casos de darle un

mal uso o no cumplir con los preceptos establecidos. Está claro que la intimidad como concepto, no puede comprenderse únicamente como se expresa en lo Constitución Política, además es necesario tener en cuenta todo el contexto social y cultural que implica para el legislador una constante evaluación de todas las conductas y fenómenos que surgen en el tiempo y que atentan contra el derecho a la intimidad.

3. **NATURALEZA DEL HABEAS DATA**: Se contempla como un derecho fundamental que permite tener acceso, actualizar y rectificar información que se almacena en bancos de datos tanto de entidades públicas como privadas. Adicionalmente, el habeas data constituye un mecanismo o garantía esencial para salvaguardar otros derechos fundamentales como el buen nombre y la intimidad entre otros, cuando se puede clamar y es oportuno, posee la capacidad de proteger, restituir o evitar que se prolongue la indebida disposición de la información intima de las personas.

   Teniendo en cuenta que el hábeas data es un derecho fundamental, aquel no puede ser suspendido por aquellos individuos encargados de su administración, su respaldo constitucional implica que es inherente a la persona para que pueda gozar de una vida digna

4. **OBJETO DE PROTECCIÓN Y MATERIA CENTRAL DEL HABEAS DATA:** Los datos personales son todos aquellos que hacen parte de y solo le conciernen a la persona, por lo tanto en relación a los administradores de bancos de datos, aquellos deben cumplir con ciertos lineamientos como que su recolección y manejo, obedezcan a fines constitucionales y se implementen medidas técnicas para garantizar su protección con el objetivo de evitar su alteración, perdida o acceso no autorizado, la seguridad de los registros a la hora de tratar la información, requiere de fines legales,

entre los cuales se encuentran directamente la protección a los derechos de honra y buen nombre entre otros, y de manera indirecta, un sin número de derechos que se pueden ver involucrados con el uso de los datos personales, aquellos siempre deben ser utilizados de tal forma que en ningún sentido logren afectar la dignidad humana, y en los casos en que se haga, no puede quedar impune aquella acción, los portadores de los datos deberán responder tanto civil como penalmente por los daños y perjuicios que resultaren como consecuencia de acciones dolosas o culposas, por lo tanto cada persona es quien decide cuales de sus datos pueden ser conservados y expuestos a la luz pública, y siempre contaran con la posibilidad de ratificarlos y actualizarlos.

5. **FINALIDAD DEL HABEAS DATA:** Su principal finalidad consiste en mantener la información intima ante la disposición incontrolada por parte de terceros, permitiéndole a su titular la herramienta jurídica de impedir que se les vincule a datos falsos, equívocos o reservados, desvirtuando así su identidad. El derecho del Habeas data cumple, entonces, la función de proteger a toda persona contra el peligro del abuso de la información, de manera que garantice autodeterminación de informativa. Por último, es posible concluir que la utilidad práctica del hábeas data se resume a poder salvaguardar la reputación y buen nombre de los ciudadanos en relación a todos aquellos casos en donde el almacenamiento de sus datos cuente con errores u omisiones que puedan alterar de una manera negativa la percepción que se tiene de ellos, así pues se pretende evitar una especie de marginación injustificada.

6. **PILARES DEL HABEAS DATA:**

- En cuanto a la propiedad del dato personal, es importante concluir que su titular es la persona que lo brinda o de quien se consigue, y no quienes fungen como

administradores de los bancos de datos, así ellos estén expresamente autorizados por su titular para dar algún uso en especial.

- Teniendo en cuenta la idea anterior, para que a un banco de datos se anexe información personal de una persona, se precisa de la autorización previa de su titular especificando los fines y condiciones para su utilización.
- Los datos personales, comprendidos como toda información concerniente a la persona, deben ser tratados de forma tal que su uso no afecte derechos fundamentales de la persona y que en todo caso se respeta la dignidad humana que se menciona en la constitución.
- La recaudación y tratamiento de datos, debe garantizar a las personas que su actuación es acorde con un fin necesario y legal, que la información es actual y precisa para el uso que se pretende y que se adoptaran las medidas adecuadas para impedir el abuso en cualquier ámbito de tal información.
- Los administradores de los bancos de datos, podrán ser civil y penalmente responsables por los daños y perjuicios que se produjeren como resultado de acciones dolosas o culposas que vulneren los derechos fundamentales de los ciudadanos.
- El titular del dato podrá tener constante acceso a su información contenida en registros de bases de datos, además podrá ratificarla y actualizarla. Los datos tienen por su naturaleza misma, una vigencia limitada en el tiempo, lo cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles que afecten negativamente a sus titulares.

BIBLIOGRAFÍA

Numeral 4, artículo 10. Decreto 1377 de 2013. (s.f.).

Angarita, C. (1993). *Corte Constitucional.* Recuperado el Mayo de 2016, de http://www.corteconstitucional.gov.co/relatoria/1993/T-008-93.htm

Artículo 28, ley 1581 de 2012. (s.f.).

Artículo 3, Ley 1581 de 2012. (s.f.). *Ley 1581 de 2012*.

BANCO INTERAMERICANO DE DESARROLLO. (2005). *Egconsgroup.* Recuperado el Mayo de 2016, de http://www.egconsgroup.com/publicaciones/HabeasDataProteccionDatos.pdf

Barón Angarita, C. (1992). *Corte Constitucional.* Recuperado el Mayo de 2016, de http://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

Bartra, J. Z. (2014). *Sisbib.* Recuperado el Mayo de 2016, de http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/human/Zelada_BJ/Introd.pdf

Bazán, V. (2005). *Redalyc.* Recuperado el Mayo de 2016, de http://www.redalyc.org/pdf/820/82030204.pdf

Beltran Sierra, A. (2004). *Corte Constitucional.* Recuperado el Mayo de 2016, de http://www.corteconstitucional.gov.co/relatoria/2004/T-846-04.htm

Certicámara. (2013). *colombiadigital.* Recuperado el Mayo de 2016, de https://colombiadigital.net/publicaciones_ccd/anexos/certicamara_proteccion_datos_ago28.pdf

Constitución Política de Colombia. (1997). Bogotá: Legis.

CONTRERAS, A. F. (2014). *Javeriana.* Recuperado el Mayo de 2016, de http://repository.javeriana.edu.co/bitstream/10554/14895/1/EscobarPenalverAndresFelipe2014.pdf

Cuadrada, E. B. (2007). *UOC.* Recuperado el Mayo de 2016, de http://www.uoc.edu/idp/5/dt/esp/bru.pdf

Estrada, A. J. (2013). *Corte Constitucional.* Recuperado el Mayo de 2016, de http://www.corteconstitucional.gov.co/relatoria/2013/t-058-13.htm

FNG. (2014). *Fng.* Recuperado el Mayo de 2016, de https://www.fng.gov.co/ES/Documentos%20%20Proteccin%20de%20Datos%20Personales/Manual%20Habeas%20Data.pdf

Greiffenstein, J. S. (1992). *Corte Constitucional.* Recuperado el Mayo de 2016, de http://www.corteconstitucional.gov.co/relatoria/1992/T-480-92.htm

HCHR. (2003). *Hchr.* Recuperado el Mayo de 2016, de http://www.hchr.org.co/publicaciones/libros/mecanismos.pdf

Hernandez, J. C. (2012). *Corte IDH.* Recuperado el Mayo de 2016, de http://www.corteidh.or.cr/tablas/r32012.pdf

Instituto de Transparencia e Información Pública de Jalisco . (2010). *Itei.* Recuperado el Mayo de 2016, de http://www.itei.org.mx/v3/documentos/estudios/estudio_habeas_data_6abr10.pdf

Medrano, M. M. (s.f.). *Biblio Juridicas.* Recuperado el Mayo de 2016, de http://biblio.juridicas.unam.mx/libros/5/2264/4.pdf

Mejía, J. C. (2008). *Habeas data: fundamentos, naturaleza, regimen.* Bogota: Universidad Externado de Colombia.

Numeral 3, artículo 10. Decreto 1377 de 2013. (s.f.).

Pinilla Pinilla, N. (2007). *Corte Constitucional.* Recuperado el Mayo de 2016, de http://www.corteconstitucional.gov.co/relatoria/2007/T-173-07.htm

Pretelt, J. I. (2014). *Corte Constitucional.* Recuperado el Mayo de 2016, de http://www.corteconstitucional.gov.co/RELATORIA/2014/T-176A-14.htm

Puccinelli, O. (2004). *Iprofesional.* Recuperado el Mayo de 2016, de http://www.iprofesional.com/adjuntos/documentos/08/0000887.pdf

Remolina, N. (1994). *Uniandes.* Recuperado el Mayo de 2016, de http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/El-habeas-data-en-Colombia-1994- R15_A4.pdf

Rojas, Y. P. (2013). *Udes.* Recuperado el Mayo de 2016, de http://service.udes.edu.co/revistas/index.php/Lex-UDES/article/P2.pdf

Ruiz, A. G. (2014). *AGPD.* Recuperado el Mayo de 2016, de https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Proteccion_de_datos_y_habeas_data.pdf

Sentencia T–522. (1997).

SIC. (2014). *Sic.* Recuperado el Mayo de 2016, de http://www.sic.gov.co/drupal/sites/default/files/normatividad/Resolucion_36863_2014.pdf

SIC. (2014). *Sic.* Recuperado el Mayo de 2016, de http://www.sic.gov.co/drupal/sites/default/files/normatividad/Concepto_14-118247.pdf

Solimano, S. M. (2011). *Egov.* Recuperado el 2016, de http://www.egov.ufsc.br/portal/sites/default/files/el_habeas_data_en_uruguay_perspectivas_a_tres_anos_de_su_instauracion.pdf

T-658. (2011).

UGC. (2015). *Ugc.* Recuperado el Mayo de 2016, de http://www.ugc.edu.co/documentos/derecho/revistas/mecanismos_de_derechos_individuales_y_colectivos_2.pdf