El Habeas Data: un conflicto de Intereses para la protección de datos en Colombia

Habeas Data: a conflict of interest for data protection in Colombia

Valeria Arroyo Montero
Valeriaam1999@gmail.com

Iván Sotelo
Ivansotelo31@hotmail.com

Valentina Medina Tejada
Vamedina389@gmail.com

Politécnico Grancolombiano
Derecho
Colombia

Resumen

En el presente artículo se lleva a cabo el estudio del tema de Habeas Data y la protección de datos que se da en Colombia, con el fin de vislumbrar que los datos personales corren riesgo de comercialización y mala fe de empresas privadas o públicas, es por ello, identificar los casos en los que se vulnera el derecho a la protección personal e identidad, intimidad de la persona, resaltando los principios que emanan del Habeas Data, de la Constitución y la Ley. Es esencial, resaltar que son muchas las entidades que comercializan ilegalmente con la información de las personas a través de casos en los que se encuentra sancionadas por la manipulación del Habeas Data sin autorización o permiso de las personas. Existen diferentes empresas que comercializan con la información y base de datos de las personas para ofrecer productos o servicios, volviéndose un dolor de cabeza para las personas la falta de control por la Superintendencia de Industria y Comercio y demás entidades comprometidas a la vigilancia y tratamiento de los mismos. Para el cumplimiento de los objetivos propuestos se implementará el método descriptivo, deductivo, con enfoque cualitativo, recurriendo a motores de búsqueda que se encuentran en repositorios de las universidades, e-brary, Dialnet, bases de datos de Superintendencia de Industria y Comercio, protección al consumidor, entre otras.

Palabras clave:

Conflicto de intereses, derecho fundamental, Habeas Data, principios, protección.

Abstract

In this article, the study of the subject of Habeas Data and the data protection that occurs in Colombia is carried out, in order to glimpse that personal data is at risk of commercialization and bad faith of private or public companies, it is for this, identify the cases in which the right to personal protection and identity, privacy of the person is violated, highlighting the principles that emanate from Habeas Data, the Constitution and the Law. It is essential to highlight that there are many entities that illegally trade with people's information through cases in which they are penalized for the manipulation of Habeas Data without authorization or permission of the people. There are different companies that trade with the information and database of people to offer products or services, becoming a headache for people the lack of control by the Superintendence of Industry and Commerce and other entities committed to the surveillance and treatment of the same. For the fulfillment of the proposed objectives, the descriptive, deductive method will be implemented, with a qualitative approach, using search engines found in university repositories, e-brary, Dialnet, databases of the Superintendence of Industry and Commerce, protection to the consumer, among others

Keywords

Conflict of interest, fundamental right, Habeas Data, principles, protection.

Recepción: Fecha de entrega 01/06/2023 Aceptación: _____ Fecha de sustentación DD.MM.AAAA

Cite este artículo como:

Apellido, A., Apellido, A. & Apellido, A. (año). Título del artículo. Working Paper FSCC, Volumen 1. [p.-p.]. doi:xxxxxxx

Introducción

El manejo del Habeas Data en Colombia es el tratamiento de datos de las personas regulado por la Constitución Política en el artículo 15 y la ley 1581 de 2012, sin embargo, se ha vislumbrado un riesgo en el tratamiento de los mismo por empresas que sin autorización se involucran con información delicada de las personas, para ofrecer diferentes productos o servicios, volviéndose un dolor de cabeza para las personas la falta de control por la Superintendencia de Industria y Comercio y demás entidades comprometidas a la vigilancia y tratamiento de los mismos.

Es fundamental, que con la presente investigación se logren identificar los riesgos y peligros de la información que hace parte también del derecho a la reserva y la intimidad, por ello, se requiere identificar los límites al derecho al acceso a la información pública, y los conflictos que se pueden suscitar frente a los malos manejos.

Por ello, como pregunta investigativa se resolverá la siguiente: ¿Cuáles son las consecuencias del mal tratamiento de la información personal "habeas data", para proteger el derecho a la intimidad como derecho fundamental en Colombia?

Conforme lo anterior se planteará como objetivos los siguientes:

El objetivo general de esta investigación es, Establecer los mecanismos sancionatorios a las entidades que hagan uso indebido de la información personal "habeas data" y la reparación a las víctimas del derecho a la intimidad como derecho fundamental.

Como objetivos específicos se establecerán los siguientes:

- Analizar los conceptos de habeas data, tratamiento normativo y principios frente al manejo de los datos personales.
- Examinar casos en los cuales se determina la existencia de la vulneración de los derechos fundamentales a la intimidad y reserva en Colombia.
- Debatir las posibles soluciones entre la resolución de conflictos frente al manejo del Habeas Data en Colombia.

Marco Jurídico Analítico

El Habeas Data en Colombia se encuentra regulado en la Constitución y la Ley.

En la Constitución Política artículo 15 manifiesta que todas las personas tienen derecho a su intimidad personal y familiar, a conservar su buen nombre, por ello, el Estado debe respetarlos y garantizar el respeto de las personas. Es una norma que manifiesta el derecho el derecho a conocer, actualizar y rectificar la información que se encuentre en base de satos de entidades públicas o 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 interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley" (Constitución Política de 1991, art. 15).

Es fundamental la anterior manifestación del legislador en el entendido que la

información no debe circular de manera irregular o ilegal, y se debe respetar la libertad de las personas para el manejo de esta.

La Ley 1266 de 2008, se encuentran disposiciones generales del Habeas Data, donde se regula el manejo y protección de información que se encuentra en bases de datos personales, financieros, crediticios, comerciales, servicios, entre otras.

Es fundamental vislumbrar que es un derecho acceder a la información de las personas asegurando que la misma sea veraz y confiable, datos que se encontrarían registrados en un banco de datos administrado por entidades públicas o privadas (Ley 1266 de 2008, art. 2).

Así mismo resaltan los principios de la administración de datos de los cuales se pueden describir así:

Principio de Veracidad o Calidad de Datos: consiste en que la información en las bases de datos debe ser exacta, actualizada, comprobable y comprensible, prohibiendo el registro y divulgación de información incompleta o parcial que induzca al error.

Principio de finalidad: consiste en obedecer una legitimidad en cuanto a la finalidad, donde busca información del titular de manera previa o concomitante con autorización de la persona.

Principio de Circulación Restringida: refiere que la información tiene unas limitaciones frente al tratamiento de datos personales, especialmente sobre la temporalidad de la información y la finalidad del banco de datos.

> "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 los usuarios autorizados conforme a la presente ley" (Ley 1266 de 2008, art. 4).

El principio de temporalidad de la información refiere que no puede ser suministrada la misma "usuarios o terceros cuando deja de servir para la finalidad del banco de datos" (Ley 1266 de 2008, art. 2).

Principio de Interpretación Integral de Derechos Constitucionales: se deben amparar los derechos constitucionales como el habeas data, el buen nombre, la honra, intimidad e información. Porque los titulares de la información deben contar con la armonía y equilibrio del derecho a la información considerado un derecho fundamental.

El principio de seguridad consiste en el debido manejo de información, que debe contar con medidas técnicas necesarias que garanticen seguridad en los mismos, impidiendo se alteren, pierdan o se consulten

o usen sin autorización (Ley 1266 de 2008, art. 2).

Principio de Confidencialidad: tanto las personas naturales o jurídicas que intervienen en la administración de datos personales que no tengan naturaleza de públicos deben garantizar en todo tiempo su reserva, así se haya finalizado su relación de labores de administración de datos, "pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma" (Ley 1266 de 2008, art. 4).

Se considera norma estatutaria la Ley 1581 de 2012, por la cual se diseñan mecanismos para proteger datos de las personas y principios importantes, que se explican así:

Principio de Legalidad: es una actividad reglada que se sujeta a la ley y la constitución.

Principio de Libertad: identifica que se ejerce con consentimiento previo, expreso e informado por el titular. Los datos personales deben contar con autorización o cuando no se cuente con la autorización se debe revelar por orden judicial.

Principio de Transparencia: se debe garantizar que el tratamiento de datos sea de manera responsable, sin abusar del derecho o de la administración de la información.

Con el Decreto 1377 de 2013 se reglamenta la Ley 1581 de 2012, donde resaltan conceptos del tema objeto de estudio, y resalta de manera fundamental la extensión a la solicitud a la Superintendencia de Industria y Comercio como responsables que deben proveer una descripción de procedimientos para la recolección, almacenamiento, uso, circulación y supresión de información, las finalidades para las cuales la información es recolectada, la necesidad de obtener la misma. Así mismo, es esencial que no se podrá utilizar medios engañosos o fraudulentos para el tratamiento de datos personales.

Método

La metodología utilizada será la descriptiva, aquellas que resalarán los elementos y características del tema objeto de estudio. Es una investigación de este carácter porque está encargada de analizar el tema a través de antecedentes normativos y estudios realizados por expertos, de relevancia para la sociedad, especialmente para las personas con el uso de información.

Para el desarrollo del presente artículo se recurrió al estudio descriptivo exploratorio, el cual tiene el objetivo de abordar las características o cualidades de un problema de investigación (Fernández, 2013; Sampieri, Collado, & Lucio, 2006).

Este trabajo corresponde a una investigación cualitativa, donde se describen causas, factores e incluso consecuencias en la situación particular (Hernández y otros, 2007).

Es una investigación cualitativa porque busca principalmente "dispersión o expansión" de los datos o información recuperadas del tema objeto de estudio, se realizara este enfoque porque su análisis partirá del análisis de las principales fuentes del derecho, sin tener que realizar una investigación de campo (Hernández, 2004, p. 12).

Así mismo también se hará una investigación con enfoque cuantitativo al identificar los casos objeto de conflicto de competencia frente a la normativa internacional y nacional. Es una investigación Deductiva porque se realiza un análisis de la normatividad y su aplicación, del análisis de casos para identificar las complicaciones existentes.

Las investigaciones deductivas tienen un procedimiento de investigación destacado por ser "un tipo de pensamiento que va desde un razonamiento más general y lógico, basado en leyes o principios, hasta un hecho concreto. Es decir, es un método lógico que sirve para extraer conclusiones a partir de una serie de principios" (Aspasia, 2023).

El principal método para razonar, concluir es la deducción, en sentido estricto y especifico es la demostración o afirmación de premisas "sobre la base de las leyes de la Lógica" (Lizardo, s.f., p. 1).

Análisis

Antecedentes del Habeas Data

El Hábeas Data es una palabra tomada del latín "Hábeas" que significa "tráigase", y Data que es traída del inglés que significa dato, es decir, que las dos palabras es obtener datos, traer datos, tener conocimientos de "datos propios en poder de otro" (Pierini, A. 2002. p.21).

Los indicios del Habeas Data fue en Estados Unidos a través de los periodistas Brandéis y Warren "quienes tenían como objetivo que se establecieran limites jurídicos para que no se permitiera la intromisión del periodismo en la vida privada de las personas, luchando así por la protección del derecho de intimidad (Conde y Fayos, 2014).

También fue influenciado por la Constitución de Alemania (1919) donde se incluyeron conceptos y acceso a datos de uso exclusivo para los funcionarios públicos (Masciotra, 2003).

> "El convenio para la protección de datos personales suscrito en Estrasburgo en el año de 1961, también se tiene como referente histórico, debido a que este buscaba ampliar su aplicación extendida a Colombia, permitiendo libertad de información a través de los estados parte" (Fernández, S, 2005).

En Colombia aparece a partir de la Constitución de 1991 en el artículo 15, como el derecho a conocer, actualizar y rectificar la información recogida en banco de datos y archivos a entidades públicas y privadas, “con el propósito de brindar no solo protección de la información sino de brindar garantías a los ciudadanos titulares de la misma cuando este les sea vulnerado o esté en riesgo de serlo” (Upegui, 2008. p. 195).

El habeas data es una figura constitucional, el derecho de toda personas a interponer acciones para amparar el conocimiento de datos, así reposen en bancos de datos destinados a proveer informes, “en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos” (Ortiz, 2001. p. 70).

El habeas data afirma que los datos personales son una clase de información relevante que se ha convertido en la protección del derecho fundamental de habeas data, y lo que refiere la Corte Constitucional:

Son aspectos de exclusividad de la persona, identifica a las mismas, la propiedad reside en el titular, situación que no restringe su obtención de manera licita.

> “iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación” (Remolina, 2012, p. 9).

El titular de la información es una persona natural o jurídica propietaria de la misma, aquella que reposa en un banco de datos, de una entidad u organización que conoce o recibe aquellos por los titulares de la información, por una relación comercial o servicio, o cualquier índole.

La fuente de información es la persona, entidad u organización que recibe o conoce datos personales de los titulares, en virtud de una relación comercial o de servicio o de cualquier índole y que con autorización legal o del titular permite conocer datos al operador e integrarlos para el usuario final. Por Ejemplo: El proveedor de servicios de comunicaciones. Si la fuente entrega la información directamente al usuario y no por el operador, tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos.

El vínculo de cualquier índole se entiende como el que se genera de una o más obligaciones de la fuente y el titular, donde se legitima a reportar la información positiva o negativa, donde se debe contar legalmente con la autorización del reporte.

> “Reporte no genera obligación alguna entre la supuesta fuente y el reclamante; será requisito indispensable la existencia de una obligación entre estos para que sea posible realizar un reporte” (Superintendencia de Industria y Comercio, s.f.).

El operador de la información es la persona, entidad que recibe la fuente de varios titulares, los debe administrar adecuadamente, y poner en conocimiento a los usuarios conforme a los parámetros de ley. Por ejemplo la “Central de Información Financiera CIFIN y Datacrédito” (Superintendencia de Industria y Comercio, s.f.).

El usuario es la persona que puede acceder a la información suministrada por el operador autorizado por el titular de la información. Por ejemplo, entidades bancarias, proveedores, entre otros.

El dato personal es la que está vinculada a una persona determinada, que se asocia a una persona natural o jurídica, datos públicos o privados o semiprivados. Son públicos cuando la ley lo determina así, los que se encuentran contenidos en documentos públicos, sentencias, registro civil, entre otros.

> El dato semiprivado es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector personas o a la sociedad en general, como el dato financiero y crediticio (Superintendencia de Industria y Comercia, s.f.).

Es esencial para el presente estudio identificar los principios en el marco del Habeas Data con el fin de perseguir el cumplimiento de los mismos por parte de empresas privadas y públicas.

Principio de Finalidad

Es la finalidad legitima del acuerdo, donde se obligan a las partes a recolectar los mismos de manera responsable, por ello, debe comunicar al titular previamente para el otorgamiento del permiso del uso, cuando sea de manera necesaria, y cuando se solicite información al respecto.

Principio de Circulación

Consiste en que los datos personales no pueden ser accesibles por internet o medios de comunicación masiva, salvo que la información sea pública, o que el acceso sea controlado.

Principio de Temporalidad

Es aquel que refiere a la perdida de necesidad de los datos, y que estos mismos deben dejar de ser suministrados por el responsable de su administración.

Principio de Interpretación de Derechos Constitucionales

Es la interpretación de las normas sobre datos personales que son amparadas por la constitución y la ley, “el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información” derechos que son la armonía del derecho a la información

(Superintendencia de Industria y Comercio, s.f.).

Principio de seguridad

La obligación de los administradores de la información para incorporar medidas que mantengan la misma segura, evitando y limitando el conocimiento de manera ilegal, adulteración, entre otras que pongan en riesgo a los titulares.

Principio de confidencialidad

La misma palabra lo refiere, y es que la administración de la misma se realiza con la obligación de reserva, donde solo se debe realizar el suministro o comunicación con las autorizaciones dadas por el titular, y la finalidad.

Protección al Derecho a la Información

Existe una política en Colombia bajo la Ley 1712 de 2014 que es la norma que asegura la transparencia y el derecho al acceso a la información pública, teniendo en cuenta que es un derecho humano obtener esta información.

El objetivo es que esta información se encuentre en posesión, custodia o bajo control de cualquier entidad pública, órgano y organismos del Estado en Colombia, persona natural o jurídica.

Las disposiciones van en vía a: fortalecer obligaciones que deben facilitar el acceso a la información, se verifican las categorías de las personas obligadas, establece derechos y deberes en materia de información y respuesta a sus solicitudes y afianzar el sistema de acceso público para el ejercicio de los derechos (Secretaria de Transparencia, 2015).

Conforme a ello, se explica un término muy importante para la presente investigación, ya que la intención es que el manejo de datos sea de manera transparente.

Transparencia es “es el “marco jurídico, político, ético y organizativo de la administración pública” que debe regir las actuaciones de todos los servidores públicos en Colombia, implica gobernar expuesto y a modo de vitrina, al escrutinio público”

Tiene tres dimensiones a observar:

a. Transparencia de la gestión pública, que implica la existencia de reglas claras y conocidas para el ejercicio de la función pública (planeación, decisión, ejecución y evaluación de programas y planes), así como de controles para la vigilancia de las mismas (Secretaria de Transparencia, 2015).

b. Transparencia en la rendición de cuentas, que conlleva la obligación de quienes actúan en función de otros, de responder eficaz y recíprocamente sobre los procesos y resultados de la gestión pública (Secretaria de Transparencia, 2015).

c. Transparencia en el acceso a la información pública, que supone poner a disposición del público de manera completa, oportuna y permanente, la información sobre todas las actuaciones de la administración, salvo los casos que expresamente establezca la ley (Secretaria de Transparencia, 2015).

Con fundamento en la transparencia, se hace necesario que se fijen procedimientos, mecanismos y herramientas para garantizar el pleno derecho del acceso a los datos personales. Porque a pesar de la regulación normativa.

Ahora bien Araujo (2009) refiere que se han encontrado problemas de índole constitucional en el tema de protección de datos, dado que al dársele el carácter de derecho ¿Por qué se constitucionaliza el derecho al acceso a la información?, interrogante que se hace Carbonell (s.f.)., y es la necesidad del Estado, entidades públicas y privadas, personas naturales que necesitan saber sobre la identidad de una persona para evitar realizar negocios con efectos irregulares, identificar antecedentes que pueden perjudicar a otros, transacción financieras, entre otros para proteger los bienes jurídicamente tutelados de las demás personas.

No obstante, surgen otros interrogantes como "¿En qué medida la información encuentra una tutela jurídica que la proteja adecuadamente cuando es objeto de utilización y disposición por quien o quienes la poseen, y que se manifieste tal acción a través de los medios de comunicación? ¿Existen las normas jurídicas suficientes que obliguen a los sujetos poseedores de esta información a proporcionarla y a protegerla?" (Araujo, 2009, p.195).

Los anteriores cuestionamientos, se han dado porque en la actualidad la información de las personas se encuentra en riesgo por delincuentes que se apropian de ella para hurtar económicamente a las personas, es decir, se dan dado delitos como la estafa, el hurto, falsedad de identidad personal, falsificación de documento público y privado, entre otros, y esto se debe a la falta de protección y manipulación por parte de las entidades que tienen el supuesto de derecho de conservar los datos de las personas.

Así mismo, se puede interpretar que la información es susceptible de apropiación por origen, y también por su origen pertenece al autor.

Es decir que se dispone para fines legales que permiten la posesión del autor e información para un verdadero derecho real, que se puede manejar por la existencia de bases de datos electrónicas, lo que permite un manejo rápido y eficaz, que puede soportar grandes volúmenes de información.

Respeto a ello, se expresa que la ciencia de información no está asegurada y titulada jurídicamente de manera suficiente, por ser una disciplina nueva que no cuenta con manipulación y conocimientos por parte de entidades públicas y privadas.

> "Por lo tanto, si la información implica un objeto de propiedad como si fuera un derecho real, al ser producto de la actividad humana, lo pertinente y apropiado es que esta ciencia de la información se encuentre regulada jurídicamente en toda su dimensión" (Araujo, 2009, p.197).

Ahora bien, es fundamental la expresión de base de datos que se popularizo en el siglo XX, a través de la evolución del mundo de la informática y la digitalización de documentación, las transacciones económicas, financieras, comerciales, intercambio de información a nivel mundial, entre otras que han sido fundamentales para el desarrollo de los países y las sociedades.

Las bases de datos se organizan de manera particular con un grupo particular de usuarios, por campos y suministro de herramientas tecnológicas que permiten la manipulación de los mismos objetivamente.

> "Una herramienta para el acceso oportuno, confiable y preciso a la información a través de la recopilación, sistematización, almacenamiento, organización y difusión de un determinado tipo de documentos" (Villanueva, 2004).

Es claro que el avance de la tecnología, produce el avance de los seres humanos, los medios de comunicación y su relación con la información, independientemente de la utilidad y beneficios que producen, es incuestionable que si no tienen un control en el manejo son un peligro individual y colectivo "el uso y disposición racionales de la información, objeto de estas bases de datos, lo más probable es que puedan causar daños a sus propietarios, cuando no exista el consentimiento para su difusión o divulgación" (Araujo, 2009, p.199).

Es importante resaltar, que el desarrollo de las tecnologías marca paradigmas que extralimitan el marco jurídico, por ello, deben modificarse o crear nuevas normas.

> "El desarrollo tecnológico de los medios de comunicación, indudablemente influyen de manera categórica en el manejo de la información, y origina grandes beneficios, pero al mismo tiempo la posibilidad de causar grandes perjuicios" (Araujo, 2009, p.199).

La regulación jurídica por ello es tan importante para la protección de datos personales, por ello en la Constitución de la Unión Europea, considerado un derecho fundamental, el Tribunal Constitucional Español en sentencia 292 de 2000, otorga claridad del carácter autónomo e independiente del derecho fundamental.

Recibe otro concepto el derecho de protección de datos personales general como el conjunto de información de una persona física, establecido en el Convenio 108 del Consejo Europeo, para la protección de datos y su tratamiento automatizado, con la

directrices de la Organización de Cooperación de desarrollo económico, los flujos trasfronterizos y directiva 95/46 del Consejo Europeo de 1995, que define los datos personales "Toda información sobre una persona física identificada o identificable (…)" (Gómez y Omelas, 2006).

Derecho a la Privacidad

Es un derecho que se define como la libertad y facultad de las personas para desenvolverse en el ámbito social, personal o familiar, conforme a sus patrones de conducta, costumbres o hábitos, y el inmiscuirse en ella debe solicitar autorización.

> "El derecho a decidir en qué medida compartirá con los demás sus pensamientos, sus sentimientos y los hechos de su vida personal, comprende los aspectos muy particulares de la identidad individual, la voz, la imagen, la edad, la nacionalidad, la salud, los hábitos sexuales, las ideas religiosas, políticas, filosóficas, la situación patrimonial, financiera; en suma, sus datos estrictamente personales" (Quiroz, 2016).

La evolución de las Tecnologías de la Información (TIC´s) da lugar al derecho de regularse jurídicamente la protección de la libertad e intimidad, "amenazados por el acopio de datos y la existencia de sofisticados sistemas de registros automatizados en entidades públicas y privadas" (Quiroz, 2016).

Los desafíos de los avances tecnológicos es la protección de la privacidad de datos de las personas, donde se hace fundamental lograr un equilibrio entre la tecnología y protección de datos personales, con la ayuda de herramientas jurídicas y tecnológicas. (Viega y Baladán, 2014, p. 180).

El derecho fundamental a tutelar es la reserva a la intimidad, donde no debe haber "injerencia por parte del Estado ni de particulares; se protege a través de la acción judicial de Hábeas Data. La base legal se encuentra en la Declaración Universal de los Derechos Humanos (1948)" (Quiroz, 2016).

En el art. 12, dispone que nadie puede ser objeto de injerencias arbitrarias que perturben la vida de las personas, intimidad, familia, domicilio, ataques a su honra o reputación.

> "Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.
> Y, en la Constitución Política del Perú de 1993" (Quiroz, 2016).

> "Artículo 2. Toda persona tiene derecho: Inc. 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.
> Inc. 7. Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviadas

> en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley" (Quiroz, 2016).

Autodeterminación Informativa

Es un derecho fundamental que se deriva del derecho a la privacidad, relacionado con el Habeas Data "es la autodeterminación informativa, que es un derecho de tercera generación, cuya característica esencial es la solidaridad, ya que para su real garantía exige la acción mutua, tanto de la persona, el Estado y las entidades públicas y privadas" (Quiroz, 2016).

> "Encontramos en la solidaridad la razón de ser de los derechos de tercera generación, como en su momento lo fue la libertad y la igualdad para los derechos de primera y segunda generación respectivamente" (Marecos, 2011, p.50).

En Alemania fue donde por primera vez apareció el concepto de autodeterminación informativa, un principio enunciado en sentencia del Tribunal Constitucional de dicho país en 1983 que sostuvo lo siguiente:

> "(…) supone la facultad del individuo de disponer y relevar datos referentes a su vida privada, en todas las fases de elaboración y uso de datos, o sea, su acumulación, su transmisión, su modificación y su cancelación" (Pulgar, 2006, p. 96).

La autodeterminación supone el derecho de acceder y controlar la información personal registrada en la base de datos donde solo se puede ejercer las facultades de:

> "a) Solicitar la corrección, rectificación, actualización o modificación de datos inexactos.
>
> b) Solicitar la cancelación de datos obsoletos, inapropiados o irrelevantes.
>
> c) Facultad de solicitar la cancelación de datos personales obtenidos por procedimientos ilegales.
>
> d) Facultad de exigir que se adopten medidas suficientes para evitar la transmisión de datos a personas o entidades no autorizadas" (Quiroz, 2016).

Faculta a los individuos a decidir qué datos son los que pueden ser o no conocidos, con autorización expresa, porque ahí se controla la información de datos de las persona, para preservar su privacidad frente al peligro que enfrentan las mismas con las TIC´s .

> "Por los que toda persona debe contar con efectivas garantías legales que protejan el tratamiento de sus datos personales. Es así que, "Las nuevas condiciones de ejercicio de los derechos humanos han determinado

> una nueva forma de ser ciudadano en el Estado de Derecho de las sociedades tecnológicas (…)" (Marecos, 2010, p. 52).

Riesgo ante el Robo de Datos Personales

La Superintendencia de Industria y Comercio (2023) permite realizar una serie de recomendaciones ante el latente riesgo de robo de datos en Colombia y en el mundo, suplantación de identidad donde se tiene la intención de cometer delitos, para adquirir productos, servicios o créditos, estafas y otros delitos de mayor gravedad aprovechándose de la comercialización de datos personales sin control por parte de las entidades públicas o privadas.

Niño (2022) ante el riesgo inminente en el tratamiento de datos en el comercio electrónico (e-comerce), auqneu ha contraído diferentes beneficios, con el paso del tiempo estos datos de carácter privado pueden llegar a ser susceptibles de manejo inadecuado.

> "Por lo tanto, se debe generar más conciencia que no todas las plataformas brindan la misma seguridad y cuidado en nuestros datos personales, ya que, cuando estamos entregando una información tan valiosa suministramos gran parte de nuestra intimidad. Sin embargo, uno de los grandes desafíos que presenta el *e-commerce* es la protección de los datos personales, porque estos pueden llegar a traspasar fronteras" (Niño, 2022).

Existen diferentes investigaciones sobre los riesgos del tratamiento de datos, y las infracciones al derecho de privacidad en transacciones que se realizan a través de las redes, sin embargo, estas se agravaron durante la pandemia reflejando que el 30% de los consumidores colombianos han sido blanco de fraude digital. "Transacciones en línea en más de 40.000 sitios web con pruebas de identidad y autenticación basadas en riesgos y análisis de fraude que desarrolla (TransUnion, 2021)".

Piñeros (2021) se refiere a los estafadores mundiales que se aprovechan del colapso de las redes digitales y "la pandemia ha sido un acelerador digital para empresas y personas que también ha conllevado un riesgo en materia de delincuencia en línea" (p. 6).

> "Eventos en los cuales los consumidores pueden llegar a ser víctima de diferentes riesgos, ya sea suplantación, fraude, robo, estafa, entre otros, situaciones que generan gran preocupación no solo para las personas afectadas si no para las empresas dueñas de los canales *e-commerce.* En el presente artículo, analizaremos la suplantación de identidad que sin duda es el delito más frecuente y por el cual se desprenden los diferentes riesgos" (Niño, 2022).

Para entender la gravedad de la suplantación se hace necesario definirla así “sustituir ilegalmente a una persona u ocupar su lugar para obtener algún beneficio” (Niño, 2022).

Que consiste en hacerse pasar por otra persona con fines ilícitos, para obtener un beneficio que en muchos casos es económico y patrimonial (Superintendencia de Industria y Comercio, 2019, p. 9).

En la suplantación se pueden caer en situaciones de e-commerce, donde surgen nuevamente cuestionamientos, cómo los delincuentes acceden a los datos personales?, información que se encuentra localizada en bases de datos de bancos, donde ingresan al sitio web, con usuario y contraseña de la víctima y por medio de inteligencia social contactan a la víctima para hacerse pasar por funcionarios de bancos y así poder tener acceso a información importante, “ya sea por medio de correos electrónicos o mensaje de texto al celular (datos que son personales)” (Niño, 2022).

Otro de los métodos sofisticados, “es por medio de un hacker, el hacker instala un malware 2 o software malicioso, por decirlo así, en el teléfono o en el computador de la víctima y ese software malicioso roba información del usuario y claves” (Niño, 2022).

El consumidor cuando entra al banco para realizar transacciones, inmediatamente el software captura la información sí que se percate de lo que está sucediendo, entonces de quien es la responsabilidad de salvaguardar la información si no es de la entidad financiera. No obstante, es la costumbre, no responder por esta clase de fraudes ya que otorgan la responsabilidad a la víctima por brindar información que el mismo banco solicita para realizar compras o pagos por las plataformas digitales.

> “Este software lo pueden introducir cuando el consumidor está navegando en páginas de noticias o en páginas de deportes, y en ese momento salen banners que indican que se ganó un teléfono, un viaje o cualquier otro premio y en el banner sale la opción de “click aquí”, y cuando da click se instala fraudulentamente el software malicioso, esto generalmente es muy susceptible cuando no se tiene un antivirus actualizado. Entonces silenciosamente se instala este software esperando que el cliente real entre a través de su computador a su cuenta bancaria, digite su usuario y contraseña y el software captura esa información, la cual será usada por el defraudador para estafar al cliente” (Niño, 2022).

Adicional a ello, los delincuentes hurtan las líneas telefónicas de usuarios que adquieren servicios de entidades públicas o privadas, suplantando al cliente real, realizando transacciones bancarias que requieren de un pin que se envía la número celular, “que la transacción es real, pasando así el defraudador un filtro de seguridad realizando robos en las diferentes cuentas bancarias” (Niño, 2022).

> "Mediante la suplantación de identidad los impostores obtienen créditos de diferentes entidades bancarias, adquieren productos o servicios en nombre de la persona suplantada por medio de las diferentes plataformas de comercio electrónico, siendo la persona inocente la más la afectada porque, en muchos casos, le toca asumir el pago de dichas obligaciones. Incluso tienen que hacer tramites dispendiosos ante las diferentes entidades bancarias para corroborar que fue una víctima de suplantación de identidad, en algunos casos debe de realizar trámites ante la Registraduría Nacional para poder corroborar que la persona es quien dice ser y no el delincuente que lo suplanto. Con esto, desde la perspectiva del Tratamiento de Datos Personales, se observa que se vulneran, por lo menos y según el caso, los principios de veracidad y seguridad" (Superintendencia de Industria y Comercio, 2019)

Conclusión

Las consecuencias del mal tratamiento de la información personal "habeas data", y la desprotección del derecho a la intimidad como derecho fundamental en Colombia, han sido las prácticas de ciberataques que se configuran en diversos tipos penales, por ejemplo, delito de todo tipo de fraudes, hurtos, suplantación, entre otros, que se cometen mediante la red.

La red es el medio para cometer esta clase de delitos de manera organizada, utilizando diversas formas de engaño o por equivocaciones mismas del ser humano. El panelista habla del Phisin que es un delito organizado a través de mensajes, recolección de datos y cajeros, cuando venden la información. Acción coordinada y organizado con ataques típicos a través del mensaje de internet para instalar el malware o virus que roba datos, aquellos que se obtienen por la violación del sistema de información de datos personales que poseen entidades públicas y privadas. ¿entonces a cargo de quien queda la responsabilidad?, normalmente siempre la dejan a cargo de las víctimas.

En la interacción del delincuente que maneja la ciberdelincuencia debe contactar al individuo mediante una URL, otra manera que es a través del robo, utilización de datos en una veta, mercado negro, entre otros. Es una práctica que se origina también de las cartas Nigerianas que son fraudes, suplantación con variación de tarifas anticipadas mediante un correo desde Nigeria que ofrece al destinatario compartir un porcentaje de millones de dólares de un funcionario de gobierno.

Con esta motivación el destinatario enviara información con detalles de banco, números de cuenta, identificación, entre otros datos importantes parta realizar transacciones ilegales. Es donde la víctima con su incredulidad permite la desviación de recursos, ataques cibernéticos con las cartas de Nigeria. En realidad este tipo de actos prometidos no existen y la victima cae con promesas de ganar dinero de manera fácil, pero terminan con pérdidas, porque usan la

información personal de la víctima vaciando cuentas bancarias y dejando saldos de crédito.

El fraude electrónico es una invasión al habeas data, donde se involucran a victimas nacionales o extranjeros, fraudes donde el dinero es el objetivo, tipos penales que se realiza a través de correo electrónico, mensaje de texto, redes sociales, entre otras que utilizan la informática, estudiados por la cibercriminología, que expone la forma de actuar de los delincuentes de manera organizadas para la obtención de dineros de manera ilegal.

Los riesgos son inminentes y se observa que exista diferentes normas y políticas para la protección de datos, sin embargo, la realidad es otra, existe las estafas mediante de empleo donde la victima expone su hoja de vida en redes o bases de datos dedicadas a reclutar trabajadores mediante ofertas, el delincuente o estafados envía una carta con logotipo de la empresa falsificado, para manipular los datos y recibir dineros a cambio de un viaje, exámenes, entre otros.

En las redes existen una diversidad de delitos en los que el fin es sacar provecho mediante el fraude, la estafa, y obtener dineros e incrementar el patrimonio de los delincuentes que se encuentran al acecho de todo tipo de información que las personas otorgan a través de engaños. Es importante, que las autoridades a nivel nacional e internacional puedan poner un límite al manejo de las Tic, y la evolución del delito en redes que afecta los derechos de las personas más vulnerables, delitos como terrorismo, sexuales, que se clasifican en grupos.

En línea con lo establecido en la ley 1581 de 2012, art. 22 la Superintendencia de Industria y Comercio es la entidad facultada para establecer el incumplimiento por parte del receptor, encargado del tratamiento o seguridad de la información de suministrado por las personas a las diferentes entidades.

Posterior al proceso de investigación y establecer la responsabilidad en el cumplimiento de los principios para el manejo de información personal se podrán imponer las siguientes sanciones.

a) Multas a personas instituciones por monto de hasta dos mil (2000) SMLV al momento en que se haga imposición de dicha sanción, dichas sanciones podrían darse de manera sucesiva en caso de que persista el incumplimiento.

b) La suspensión de toda actividad que implique la recolección y tratamiento de datos por un término de hasta seis (6) meses; en subsidio con esta suspensión la entidad deberá implementar las recomendaciones de la entidad para evitar la reincidencia de conductas que afecten el tratamiento de los datos personales.

c) De demostrar la responsabilidad se decretará el cierre temporal de toda actividad relacionada con la recepción y tratamiento de datos, una vez terminado este tiempo y no se hallan aplicado los correctivos se procederá a:

d) Cierre inmediato y definitivo de actividades relacionadas con la recepción y tratamiento de información persona.

Las sanciones establecidas en la ley 1501 de 2012 tendrán aplicabilidad para personas o entidades del sector privado; en el caso de presentarse incumplimiento de la norma por entidades de carácter público la Superintendencia de Industria y comercio procederá a informar a la Procuraduría General de La Nación quien es la entidad que regula el comportamiento y actual de funcionarios y entidades públicas.

Luego de revisar y analizar el origen y evolución de la ley "Habeas Data "en Colombia consideramos que si bien existe la entidad encargada e regular, investigar y sancionar las entidades que incumplían la aplicabilidad de esta norma, consideramos que hace falta implementar un proceso de información y cultura respecto a cómo cada ciudadano autoriza de manera expresa a entidades y personas la recepción y tratamiento de su información personal. En lo corrido de los años 2019 a 2023 se ha evidenciado un avance en el comercio electrónico lo que implica que con más frecuencia los ciudadanos estarán en contacto con entidades que soliciten su información por lo cual las entidades regulatorias deben trabajar en campañas que permitan a la ciudadanía estar informado sobre sus derechos sobre la información personal y su tratamiento.

Referencias bibliográficas

Carbonell, Miguel. (2006). "El derecho de acceso a la información como derecho fundamental".

Gómez, R A. Núñez, O L. (2006). Protección de datos personales en México: el caso del Poder Ejecutivo Federal, unam, México, 2006. https://www.redalyc.org/pdf/2932/293222963009.pdf

Gutiérrez, J. D., & Cure, F. D. (2020). Protección de los datos personales en el comercio electrónico: Análisis sobre las últimas decisiones y directrices de la Superintendencia de Industria y Comercio.

Marecos, A. (2011). La protección de datos personales como núcleo del derecho fundamental a la autodeterminación informativa. Una mirada desde el derecho español y europeo.

Pauner, C. (2014). Derecho a la información. Valencia, Tirant Lo Blanch.

Pérez, A. (1990). Del hábeas corpus al hábeas Data. Informática y derecho, pp. 153-161. Recuperado de http://egov.ufsc.br/portal/sites/default/ files/6_16.pdf

Pulgar, N. (2006). El hábeas data en la protección de datos y el resguardo de la intimidad del trabajador. Maracaibo, Universidad de Zulia. Facultad de Ciencias Jurídicas y Políticas. +Informe final de trabajo de grado para optar el título de magíster scientiarium en derecho laboral y administración del trabajo.

Robledo, G A. Ornelas, N Lina. Ornelas Núñez. (2006). Protección de datos personales en México: el caso del

Poder Ejecutivo Federal, unam, México.

Villanueva, E. (2006). Derecho de la información, Cámara de Diputados-Universidad de Guadalajara-Porrúa, México.

Viega, M. y Baladán, F. (2014). Protección de datos personales en América Latina. Ampliando horizontes.

Uruguay, Agencia para el Desarrollo de Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC)

Normatividad

Leyes

Ley 0527 1999.
Ley 1480 de 2011.
Ley Estatutaria 1581 de 2012.

Jurisprudencia

Corte Constitucional. (2011). Sentencia C-748-11 M.P. Jorge Ignacio Pretelt Chaljub.

Corte Constitucional. (2019). Sentencia T-610-19 M.S. Reyes Cuartas José Fernando.

Recuperado el 7 de septiembre de 2021, de Avante Abogados website: Recuperado el 7 de septiembre de 2021, de Avante Abogados website: https://avanteabogados.com/2020/03/13/proteccion-de-los-datos-personales-en-el-comercio-electronico-analisis-sobre-las-ultimas-decisiones-y-directrices-de-la-superintendencia-de-industria-y-comercio/ [Links]

López Jiménez, D. (2011). Los códigos de conducta como solución idónea frente a la elevada desprotección de la privacidad en Internet. Revista de Derecho Comunicaciones y Nuevas Tecnologías, (6), 4-21.

Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio. (2019a). Resolución 1321 de 2019: Por el cual se imparten órdenes dentro de una actuación administrativa. Recuperado de https://www.sic.gov.co/sites/default/files/files/Noticias/2019/Res-1321-de-2019.pdf

Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio. (2019b). Resolución 9800 de 2019: Por el cual se impone una sanción y se imparten órdenes. Recuperado de https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE9800-2019(1).pdf

Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio. (2019c). Resolución 21478 de 2019: Por medio de la cual se imparten órdenes dentro de una actuación administrativa. Recuperado de https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/Res%2021478.pdf

Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio. (2021). Resolución 11511 de 2021: Por la cual se impone una sanción administrativa y se imparte una orden. Recuperado de https://www.sic.gov.co/sites/defa

ult/files/estados/042021/RE11511-2021.pdf

Superintendencia de Industria y Comercio. (2021a). Manejo de información personal, “Habeas data”. Recuperado el 5 de septiembre de 2021, de Manejo de información personal, “Habeas data” website: Recuperado el 5 de septiembre de 2021, de Manejo de información personal, “Habeas data” website: https://www.sic.gov.co/manejo-de-informacion-personal

Superintendencia de Industria y Comercio. (2021). Protección de datos personales. Recuperado el 25 de agosto de 2021, de Superintendencia de Industria y Comercio: Protección de datos personales website: Recuperado el 25 de agosto de 2021, de Superintendencia de Industria y Comercio: Protección de datos personales website: https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Superintendencia de Industria y Comercio. (2021c). Protección de datos personales: Preguntas frecuentes. Recuperado el 6 de septiembre de 2021, de Recuperado el 6 de septiembre de 2021, de https://www.sic.gov.co/preguntas-frecuentes-pdp

Superintendencia de Industria y Comercio. (s/f-a). Cartilla: Formatos modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus Decretos Reglamentarios. Recuperado de https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_formatos_datos_Personales_nov22.pdf

Superintendencia de Industria y Comercio. (s/f-b). Guía para la implementación del principio de responsabilidad demostrada (Accountability). Recuperado de https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Superintendencia de Industria y Comercio. (s/f-c). Protección de datos personales: Aspectos prácticos sobre el derecho de hábeas data. Recuperado de https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Aspectos_Derecho_de_Habeas_Data.pdf

Superintendencia de Industria y Comercio: Delegatura para la protección de datos personales. (2019). Guía sobre el tratamiento de datos personales para fines de comercio electrónico. Recuperado de https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico(1).pdf

TransUnion. (2021). 206% aumentaron intentos de fraude digital originados desde Colombia. Recuperado el 30 de agosto de 2021, de TransUnion website: Recuperado el 30 de agosto de 2021, de TransUnion website: https://noticias.transunion.co/206-aumentaron-intentos-de-fraude-digital-originados-desde-colombia/