UNIVERSIDAD PONTIFICIA BOLIVARIANA

La protección de los datos en las empresas comerciales.

Valentina Tamayo Bohórquez

FACULTAD DE CIENCIAS POLITICAS Y DERECHO

DERECHO

Septiembre de 2017

La protección de los datos en las empresas comerciales.

Resumen

El derecho de habeas data es un mecanismo, el cual se ha reglamentado con el fin de que las personas puedan tener una protección de sus datos, siendo un instrumento que garantiza la defensa de los derechos humanos, permitiéndole a cualquier persona natural o jurídica conocer, acceder, actualizar, rectificar, eliminar o anular cualquier información que de ella se promulgue o que repose en un banco de datos.

En donde se requiere a su vez que además de una legislación y un sistema jurídico más riguroso, se sigan las indicaciones de las autoridades para evitar este tipo de casos, debido a que el avance tecnológico y la masificación del internet hará que cada vez más los datos personales estén expuestos, las empresas deben dar el manejo necesario, y que el tratamiento de esta información, cumpla con la finalidad en donde se "Obliga a que las actividades de recolección de datos personales obedezcan a una actividad legítima de acuerdo con la constitución y la ley. Dicha finalidad debe ser comunicada al titular de la información y es necesario obtener de este dicha autorización". (SIC)

Palabras claves: datos personales, protección, tratamiento, confidencialidad.

INTRODUCCIÓN.

La construcción de un mundo globalizado se ha venido dando por la consolidación del capitalismo y de una revolución tecnológica que a diario tiene la necesidad de tener mayor expansión mundial. Por lo tanto, se considera importante que en esta inmersión tecnológica, se le dé un buen uso al manejo de la información, teniendo la necesidad de crear una reglamentación para que dicha información no afecte ni vulnere los derechos fundamentales.

El derecho de habeas data es un mecanismo, el cual se ha reglamentado con el fin de tener una protección de datos, ya que, es un instrumento que garantiza la defensa de los derechos humanos, permitiéndole a cualquier persona natural o jurídica conocer, acceder, actualizar, rectificar, eliminar o anular cualquier información que de ella se promulgue o que repose en un banco de datos. Según la ley estatutaria 1581 de 2012, mediante la cual se dictan disposiciones generales para la protección de datos personales, el artículo 5º reza: "*Datos sensibles***.** Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garantice los derechos y las garantías de los partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.".

En el caso concreto de las empresas comerciales, este control se ha venido haciendo a través de la exigibilidad de manuales en donde se explica y se trazan los lineamientos generales

corporativos que se tienen en cuenta a efectos de proteger los datos personales de los titulares, con la finalidad de la recolección de la información, derechos de los titulares, área responsable de atender las quejas y reclamos, así como los procedimientos que se deben agotar para conocer, actualizar, rectificar y suprimir la información.

Se realizó una práctica corporativa en la empresa Almacenes Flamingo S.A, empresa que se caracteriza por las ventas a crédito, que cuenta con sedes a nivel nacional y con un portafolio que ofrece todo tipo de productos, teniendo en cuenta que por tratarse de ventas a crédito se le hace mayor exigencia en el manejo de las bases de datos, en donde se pudo evidenciar la importancia que tiene toda empresa comercial, de manejar un manual en donde se tracen los lineamientos que se tienen en cuenta para proteger los datos personales de los ciudadanos, en este caso, de los clientes, codeudores, fiadores y referencias, que confían en la entidad desde el momento que se acercan a ella y suministran su información.

DESARROLLO JURISPRUDENCIAL

En Colombia el desarrollo del habeas data, también conocido como derecho a la libertad informática o autodeterminación informática, ha estado impulsado principalmente por la Corte Constitucional. Aunque en principio se consideraba que el habeas data se limitaba únicamente a datos financieros, la Corte Constitucional en sentencia T-176A/14 especifica los principios y reglas que debe seguir el administrador de bases de datos, esta Corte en materia de habeas data ha sido constante en precisar que la administración de toda base de datos personales está sometida a los llamados principios de administración de datos personales. Entre los mencionados principios de la administración de datos personales se encuentran: los principios de finalidad, la necesidad, la utilidad y la circulación restringida, los cuales prescriben una serie ineludible de deberes en relación con las actividades de recolección, procesamiento y divulgación de la información personal.

La constitución política de 1991 en su artículo 85, trajo un listado de derechos que agrupo bajo el término “derechos de aplicación inmediata”, siendo los derechos que no requieren previo desarrollo legislativo, ni reglamentación de ningún tipo para su eficacia directa, ni condiciones para su ejercicio, por lo que son exigibles en forma directa e inmediata. En este artículo se alude al artículo 15 de la constitución que hace referencia al derecho de habeas data, el cual lo define como “el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas" siendo un derecho fundamental, de aplicación inmediata, el cual está

integrado por el derecho a la libertad y a la autodeterminación informática en general, y por la libertad económica en particular.

En la sentencia T-414 de 1992 del Magistrado Ponente Ciro Angarita Barón, la Corte Constitucional consideró el derecho de habeas data como un desarrollo específico al derecho de la intimidad y como una garantía del mismo, este consiste en "la facultad de disponer de la información y de preservar así la propia identidad informática, es decir, de permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás" (Baron, 1992), esto con el fin de contrarrestar los efectos del poder informático de tal forma que los individuos puedan tener el control sobre la información que se divulga sobre ellos y de corregir dicha información de ser necesario.

Otra sentencia es la 082-1995 del magistrado ponente Jorge Arango Mejía, que considera el derecho de habeas data como un derecho autónomo donde se afirma que: "La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación de conformidad con las regulaciones legales". (Sentencia SU 082-1995, 1995).

Es así como el 31 de diciembre de 2008 entra en vigencia la ley 1266 llamada "Ley de habeas data", la cual regula las disposiciones generales del habeas data y del manejo de la información contenida en las bases de datos y el acceso de las personas a ella, de tal manera que las personas puedan conocer, actualizar y rectificar la información que sobre ellas se haya recogido en bancos de datos tanto de entidades públicas, como privadas.

Desde su expedición se buscaba el control del manejo dado a las bases de datos de información de las centrales de riesgo, con la finalidad de proteger a los más vulnerables que en este caso, son los ciudadanos. Además, se ocupa de definir los conceptos básicos que permiten explicar quiénes son las partes en dicha relación y distinguir entre los diferentes tipos de

información. Esta ley fue la primera regulación de habeas data en el país, "es una norma de carácter parcial, ya que, su ámbito de aplicación esta sectorizado a datos comerciales, financieros, de servicios y provenientes a terceros países" (Pont, 2015).

Posteriormente, otra línea jurisprudencial de la Corte Constitucional en sentencia C-748 de 2011, reconoce que en el interior de sus miembros surgieron tendencias interpretativas en donde algunos de ellos "consideraban el habeas data como una manifestación del libre desarrollo de la personalidad, donde este tiene su fundamento último en el ámbito de la autodeterminación y libertad que el ordenamiento jurídico le reconoce al sujeto como condición indispensable para su desarrollo de la personalidad". Considerándose que el habeas data se entiende no solo como un derecho fundamental, sino que además, es polisémico, ya que, también es considerado como una manifestación de otros derechos y como una garantía misma de los demás.

En sentencia SU 458 de 2012 la Corte Constitucional reconoce una posición que desde la sentencia SU 082-1995, se había propuesto y era que: "el habeas data es un derecho autónomo y tiene un objeto protegido concreto: el poder de control que el titular de la información puede ejercer sobre quien administra la información que le concierne". Esta sentencia establece, además, la posibilidad de que en ciertos casos sea posible hablar de imputación de responsabilidad frente a quien actúa como responsable o encargado de los datos personales, y no solo como derecho fundamental que se tiene.

Con el advenimiento de la ley estatutaria 1581 de 2012 se habló formalmente de la implicación de las bases de datos y de su contenido y se propendió por la consagración de los derechos fundamentales a la intimidad, buen nombre y el habeas data, de tal manera que, en palabras de Nelson Remolina Angarita, esta ley "No es una ley para solo proteger la información

personal, sino, principalmente, para exigir un tratamiento adecuado de los datos de las personas de manera que no se lesionen sus derechos y libertades". (Remolina Angarita N. 2012)

A diferencia de la ley de habeas data, esta ley persigue la protección de datos personales registrados en cualquier base de datos, por tanto, las entidades sin importar que sean públicas o privadas se encuentran en obligación de realizar una revisión en el uso de los datos personales contenidas en sus bases, de tal forma que replanteen, de ser necesario, sus políticas de manejo de información y las herramientas que tienen implementadas para ello. Debido a que es una ley que genera no solo derechos a sus titulares sino que a su vez consagra obligaciones para los responsables del manejo de dicha información, que en este caso, son las entidades dueñas de las bases de datos.

La Corte Constitucional en sentencia T- 176 A del 2014 definió el derecho de habeas data como "El derecho *fundamental que habilita al titular de información personal a exigir, de la administradora de sus datos personales, una de las conductas indicadas en el artículo 15 de la Constitución: "Conocer, actualizar, rectificar, o una de las conductas reconocidas por la misma Corte como pretensiones subjetivas de creación jurisprudencial: autorizar, incluir, suprimir y certificar. La facultad de suprimir de las bases de datos información personal, no es de carácter absoluta, ni procede en todo momento ni circunstancia. Por el contrario, se trata de una facultad que únicamente se activa cuando el administrador de las bases de datos ha quebrantado uno de los principios de la administración de datos""*. (Sentencia , 2014)

La Asamblea Nacional Constituyente, no desarrolló a profundidad el contenido y alcance de este derecho, por lo que el Gobierno le propuso un texto que serviría como concepto del derecho de habeas data en la Constitución: "Toda persona natural o jurídica tendrá acceso a información sobre sí misma, salvo que la seguridad del Estado exija mantener la reserva, en los

casos que establezca la ley. Toda persona tiene derecho a que ella no sea destinada a un fin distinto para el cual hubiere sido suministrada. La ley reglamentará el uso de la información y de otros avances tecnológicos para garantizar la intimidad personal y familiar y el pleno de otros derechos. (Muñoz E. 1997)

Esta iniciativa estaba justificada en el hecho de que la tecnología había permitido el acceso a la información personal de manera fácil y ágil, poniendo en riesgo los derechos fundamentales y partiendo del hecho que en otros países algunos bancos de datos ya habían vulnerado los derechos fundamentales, por lo que se debía aprender de errores pasados. Además, porque al regular este tema se evitaría que el individuo perdiera el control sobre su información y estuviera informado sobre la información que sobre sí mismo se divulgaba y tuviera la facultad de corregir y eliminar toda información falsa.

Por último, la doctrina extranjera ha tratado el contenido del habeas data de forma más amplia, considerando que cobije el derecho a acceder a la información, a la actualización, a la rectificación o cancelación, a la inserción como también el derecho a conocer qué información relativa a cada persona ha sido suministrada a terceros. (Bergel, Salvador D. (2002).

Así pues, se evidencia cómo las diferentes posiciones tienen algo en común, y es que todas definen el derecho de habeas data como la posibilidad que tienen las personas de conocer, actualizar, rectificar la información que sobre ellas posee una persona o entidad, con el fin de evitar que se divulgue información falsa o improcedente que termine por ocasionar un perjuicio.

BASE DE DATOS

El profesor Mario G. Losano, precursor de la informática jurídica en Italia, define un banco de datos como "Un conjunto de informaciones que se refieren a un sector particular del conocimiento, las cuales pueden articularse en varias bases de datos y ser distribuidas a los usuarios de una entidad que se ocupa de su constante actualización y ampliación" (Losano M. 1985)

Hay infinidades de definiciones de bases de datos, pero de manera amplia y general, una base de datos se define como: "Una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular". (leon, 2011).

Desde sus inicios, estas bases se convirtieron en una herramienta fundamental de control y de manejo de las operaciones comerciales, pocos años después de su creación, grandes empresas y negocios empezaron a almacenar información en diferentes fuentes de datos y se dieron cuenta que dicha información podría tener un fin útil si eran incluidas dentro de sus operaciones y si eran unificadas en un solo lugar. Los datos personales son de gran importancia tanto que tienen gran fuerza en la económica mundial, para Ernesto Barrera significa que "Las bases de datos son las fuentes de ventajas competitivas dentro de la economía digital, en donde se identifican grupos homogéneos y se pueden realizar ofertas adecuadas a cada segmento de mercado e inclusive que sean personalizadas, construyendo de esta manera la historia de cada cliente, y teniendo presente sus preferencias en cuanto a productos y servicios que han comprado, volúmenes históricos, precios y beneficios otorgados, analizando el uso del crédito rotativo mensual, en las compras del

cliente, su información demográfica como son la edad y los ingresos principalmente, la información pictográfica en cuanto a las actividades, los intereses y las opiniones frente a su experiencia de compra y lo más importante, cuáles son los clientes rentables" (Barrera, 2012).

De acuerdo a la evolución que ha tenido el mercado y analizando que ahora se está teniendo también gran movimiento en cuanto a compras online, teniendo el e- commerce un mayor crecimiento, se evidenció la necesidad de crear la Ley 1581 de 2012 y posteriormente el decreto 886 de 2014, los cuales buscan proteger el derecho que tienen los ciudadanos a que su información no sea utilizada con fines comerciales sin su autorización, y establecen la obligación a entidades comerciales de responder a la solicitud de rectificación de información hecha por los ciudadanos. Para lograr lo anterior, reglamentan el manejo de bases de datos de todas las empresas comerciales y de las personas naturales que tengan en su poder bases de datos, el registro que deben aportar las mismas a la Superintendencia de Industria y Comercio, las políticas del tratamiento que deben dar a la información contenida en las bases ya que el incumplimiento, acarrea sanciones no solo monetarias sino también legales. En dicho registro, se debe especificar el responsable de tratamiento de los datos, los canales que ofrecen para que los titulares ejerzan sus derechos de ser necesario, finalidad de las bases de datos y el tratamiento que se le darán a los mismos.

Esto con excepción de bases que tengan por finalidad la seguridad y defensa nacional, al igual que el control y seguimiento del lavado de activos o financiamiento al terrorismo que como tal no es objeto de tratamiento en este trabajo.

AUTORIZACIÓN

Según la Real Academia de la Lengua Española autorizar significa "Dar o reconocer a alguien facultad o derecho para hacer algo", y según la Superintendencia de Industria y Comercio, en temas comerciales, la autorización consiste en "el consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior".

De esta manera una compañía al momento de recolectar datos personales debe solicitar la autorización a los titulares y para ello debe adoptar los procedimientos pertinentes informando siempre sobre las finalidades específicas del tratamiento para los cuales se obtiene dicho consentimiento y el cual puede obtenerse por cualquier medio escrito, físico o electrónico que permita su consulta posterior, por lo tanto, sin previa autorización y que se dé de manera voluntaria por el titular bajo ninguna circunstancia se puede realizar un manejo de datos e información importante, implementando para tal efecto, medidas claras sobre confidencialidad y privacidad de datos personales. Teniendo en cuenta que esto se encuentra establecido en el decreto 1377 de 2013 en su artículo 5 estableciendo que las empresas son las responsables de dar un buen manejo a este procedimiento y tener una recolección adecuada de los datos de cada cliente.

En el caso de almacenes Flamingo S.A. al momento de recolectar datos personales, se debe usar el protocolo de autorización, para que en el documento correspondiente el titular corrobore dicho consentimiento de autorización sin que eso implique la violación a los principios de información y confidencialidad. La autorización de los titulares podrá manifestarse por escrito, de forma oral o mediante conductas inequívocas, que permitan inferir de forma razonable que fue

otorgada la autorización, además, se debe almacenar dicha autorización como efecto de prueba dado el caso de que se presente una reclamación.

Lo anterior, no obsta para que los titulares de la información en cualquier momento soliciten la supresión de sus datos y revoquen la autorización otorgada en un principio para el tratamiento de sus datos. Articulo 9 decreto1277. Debido a que hay casos en los que no es necesario la autorización por parte de los titulares, como en el caso de la información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, datos de naturaleza pública y en los caso de urgencia médica o sanitaria. En estos casos el tratamiento de información es autorizado por la ley para fines estadísticos o científicos. "Casos que no son objeto de estudio para este trabajo por lo que no se desarrollaran". (Artículo 10 ley 1581)

PROCEDIMIENTO

Una empresa comercial, a la hora de realizar el manual, debe establecer el procedimiento interno adecuado para el manejo de la información contenida en las diferentes bases de datos que tengan en su poder. Así como el procedimiento externo que deben realizar los titulares de la información a la hora de solicitar alguna corrección, modificación o supresión de la misma, y de esta manera, se respetan los procedimientos y se realiza la conservación o la supresión de los datos personales que tengan en su poder.

El artículo 13 del Decreto 1377 de 2013, establece: las políticas de tratamiento que se debe dar a los datos contenidos en bases de datos por parte de las entidades comerciales y los encargados responsables de que dicho tratamiento deben cumplir conforme a lo establecido por la

ley. Dichas políticas deben constar en medio físico o electrónico y deben estar redactados en una forma clara y sencilla que permita su fácil comprensión, ya que, está se encuentra dirigida a los titulares de la información para que en un momento dado sean conocedores de lo que realizara la entidad y la finalidad de la recolección de sus datos.

Flamingo realiza la recolección de los datos personales a través de los almacenes y los canales alternativos implementados por la organización a través de un software debidamente licenciado, el cual es suministrado por proveedores especializados, dicha actividad es realizada con la autorización previa, expresa e informada del titular.

En el caso de que el titular desee que se suprima, se modifique o se corrija alguna información, se debe presentar personalmente al almacén, en donde con el documento de identidad original, descripción de sus hechos, dirección de notificación y documentos que den soporte de su reclamación podrá realizar la solicitud verbal o por escrito a través del formato de Peticiones, quejas y reclamos, como se encuentra establecido en el artículo 15 de la ley 1581. Dicha reclamación será recibida por el auxiliar de información o en ausencia de este, por el auxiliar de servicio al cliente para que sean ellos quienes queden encargados de remitir la solicitud al área responsable, quien debe dar respuesta al titular en el término establecido por la ley para ello. Si falta alguno de los requisitos mencionados, se hace necesario requerir al titular dentro de los 5 días hábiles siguientes y subsane las fallas, y si este no se pronuncia dentro de los dos meses siguientes se entenderá que ha desistido del reclamo.

Cuando el titular realiza una consulta de su información personal, almacenes Flamingo S.A cuenta con un plazo máximo de 10 días contados a partir de la fecha en que la recibe, plazo que solo se extiende por 5 días hábiles más en los casos donde no es posible atender la consulta

dentro del término inicialmente pactado y de lo cual se debe avisar al titular explicando la demora.

Es importante que los titulares agoten este procedimiento antes de instaurar la queja ante la Super Intendencia de Industria y Comercio. Además, es importante aclarar que la solicitud de supresión de información y la revocatoria de la autorización, solo surtirá efectos cuando el titular se encuentre a paz y salvo con la entidad, es decir, la misma no procederá cuando el titular tenga un deber legal o contractual con la empresa.

FINALIDAD DEL TRATAMIENTO

Los tratamientos deben tener una finalidad basados en el principio, a través del cual "Obliga a que las actividades de recolección de datos personales obedezcan a una actividad legítima de acuerdo con la constitución y la ley. Dicha finalidad debe ser comunicada al titular de la información y es necesario obtener de este dicha autorización". (SIC).

Adicional, tal como lo establece el decreto 1377 de 2013 en su artículo 4, la recolección de datos debe limitarse a los datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados, esto deber ser descrito y explicado tal como lo exige la Superintendencia de Industria y Comercio al titular de la información, para garantizar que su consentimiento sea libre y voluntario dado que entiende lo que hace y para qué se hace.

En el caso de Almacenes Flamingo los datos personales de los titulares son recolectados en desarrollo de su objeto social, con la finalidad de realizar campañas de publicidad y mercadeo para ofrecer descuentos y promociones de productos o servicios propios o de terceros,

implementar programas de fidelización, preparar estudios de mercado que le permitan establecer preferencias de consumo o determinar hábitos de pago.

Así mismo para realizar estudios de crédito, cobranza o riesgo crediticio y adelantar convenios comerciales, eventos o programas institucionales directamente o en asocio con terceros. También verificación de datos a través de consulta de bases de datos públicas o centrales de riesgo, actividades de georreferenciación y estudios estadísticos, enviando información sobre actividades desarrolladas por la compañía o envió de información que se considere de interés a través de diferentes medios.

Lo anterior se justifica puesto que Flamingo es una compañía cuyo objeto social principal es el de adquirir, almacenar, empacar, reempacar, distribuir en general y vender bajo cualquier modalidad comercial, que incluye la financiación, toda clase de mercancías, artículos y productos nacionales y extranjeros, aptos para su comercialización en centros o establecimientos comerciales departamentalizados u organizados como un conjunto de secciones o almacenes especializados.

DERECHOS DEL TITULAR

Teniendo en cuenta que los titulares de los datos personales son personas comunes y corrientes, estableciendo mecanismos sencillos y agiles para que dichas personas puedan acceder a sus datos y ejercer sus derechos sobre los mismos. Consulta que se realiza de forma gratuita por parte de las entidades en donde reposan las bases de datos, al menos una vez al mes o cada vez que se realicen modificaciones sustanciales a las políticas de tratamiento respecto a datos personales. Excepcionalmente, podrá tener algún costo en los casos donde el titular de la

información realice más de una consulta mensual, evento en el cual el titular y dueño del dato deberá cubrir los gastos referentes a envío, reproducción y certificación de documentos. Articulo 21 decreto 1377 de 2013.

Esta solicitud la puede realizar el titular de los datos personales por diferentes medios, sea presencialmente acercándose a cualquiera de los almacenes en cualquier ciudad, vía correo electrónico o inclusive a través de la línea de atención al cliente por medio telefónico.

De conformidad con el art. 8 de la Ley 1581 de 2012, el titular de los datos personales tendrá los siguientes derechos:

- El titular debe conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del mismo, este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley.
- Ser informado por el responsable del tratamiento o el encargado del tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones que se encuentre dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen.
- Revocar la autorización o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria o

supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a esta ley y a la Constitución.

- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

De conformidad con el art. 20 del Decreto 1377 de 2013, el ejercicio de los Derechos antes mencionados podrán ser ejercidos por, el titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable, por sus causahabientes, quienes deberán acreditar tal calidad, por el representante o apoderado del titular, previa acreditación de la representación o apoderamiento, o por estipulación a favor de otro o para otro.

DEBERES DEL RESPONSABLE DEL MANEJO DE INFORMACIÓN

De conformidad con el art. 17 de la Ley 1581 de 2012, el responsable tendrá los siguientes deberes como son: garantizar al titular en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data, solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el titular, informando debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada, conservando la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, garantizando que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible, actualizando la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente

le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada, rectificando la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento, suministrando al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley, exigiendo al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular, tramitando las consultas y reclamos formulados en los términos señalados en la presente ley, adoptando un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos, y por ultimo informando al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

En este sentido la fuente debe garantizar al titular de la información que sus datos personales en manos del operador son veraces, completos, exactos y comprobables, así mismo debe garantizar que cuenta con los mecanismos necesarios para que dicha información este permanentemente actualizada y rectificada, informando a solicitud del titular sobre el uso dado a sus datos y a su vez informando a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

Esto con la finalidad de que dado el caso de que se presente una reclamación, los responsables del tratamiento sean capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que implementaron las medidas apropiadas y efectivas para la recolección de los datos del titular. Es decir, cuando la Superintendencia les solicite que demuestren tal procedimiento, los responsables deberán suministrar a esta una descripción de los procedimientos

usados para la recolección de los datos personales, como la descripción de las finalidades para las cuales dicha información fue recolectada y la forma en que se realizó dicha recolección.

VIGENCIA DE LA POLITICA DE TRATAMIENTO

Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo, la cual impone a los responsables o administradores de bancos de datos la obligación de realizar una actualización permanente a fin de no poner a circular perfiles de personas virtuales que afecten negativamente a sus titulares. Esto debido al hecho de que los datos personales no tienen una vigencia infinita, sino que por el contrario, tienen una duración de tiempo razonable y necesaria, de acuerdo con la finalidad para lo cual fueron solicitados y recolectados, ya que una vez que expira o se cumpla la finalidad los responsables del tratamiento deben proceder a la supresión de los datos que tengan en su posesión.

Así las cosas, en los casos de las informaciones negativas que reposen en un banco de datos, no tienen vocación de perpetuidad por lo que después del pasado el tiempo que la ley estipula para ello, deben desaparecer. La Corte Constitucional afirma que la finalidad de la prescripción es la de clarificar la existencia o inexistencia de un derecho a partir de la actividad o inactividad de su titular durante un lapso de tiempo por lo anterior si ya transcurrió el tiempo establecido por la ley para la prescripción de la permanencia en el o inclusive, un tiempo mayor debe desaparecer dicha información.

CONCLUSIÓN

El proceso constitucional de habeas data, su alcance y determinación como derecho fundamental, ha sido largo y dispendioso en el tiempo y ha sido producto de un gran desarrollo jurisprudencial y constitucional sobre la materia. Pero aun así, hoy por hoy se puede afirmar con certeza que no ha dado los frutos esperados, ya que, las personas no tienen entero conocimiento de la aplicación de dicha ley y de los derechos que pretende proteger la misma. Evidencia de ello es que la ley 1266 de 2008 resultó insuficiente para garantizar y proteger efectivamente los datos personales por lo que fue necesario que el legislador adoptara a través de la ley 1882 de 2012 un marco jurídico autónomo y especializado que propenda por la real protección de la información.

El desarrollo de tecnologías en cuanto al manejo de información, la ampliación de la aplicación y utilización de información personal en bancos de datos, llevó a la necesidad de configurar mecanismos, límites y garantías para determinar el ámbito de protección del derecho fundamental de habeas data, de tal forma que se tengan los mecanismos jurídicos de protección adecuados para garantizar que la regulación de este derecho no sea un formalismo vacío sin contenido y así regular y sancionar conductas abusivas en este tema que pongan en riesgo o vulneren derechos fundamentales.

Debido a que el derecho del habeas data le permite a los ciudadanos no solo conocer la información que terceros tienen sobre ellos, sino además, cuál de esta divulgan, buscando con esto evitar abusos por parte de los administradores de dicha información y permitir que los titulares puedan defenderse en caso de verse afectados por registros negativos o falsos, teniendo en cuenta que un dato divulgado de la manera incorrecta y con la información equivocada puede afectar seriamente a una persona.

La diferente regulación y normatividad que ha venido surgiendo sobre el tema de habeas data y bases de datos, le ha puesto la obligación a las diferentes entidades y empresas comerciales de crear manuales y tener toda una regulación en cuanto a la recolección de información personal de sus clientes, proveedores y demás, dado que el no hacerlo puede llevar a sanciones no solo monetarias sino legales.

La protección de los datos personales no debe ser solo responsabilidad de quien solicita la información, todo esto también depende de quien brinda cada uno de los datos pues es su obligación saber, cómo, cuándo, dónde y en manos de quién, está dejando su información, además, porque muchas veces no solo se dan datos de una sola persona sino también la de su núcleo familiar poniendo en riesgo su integridad. Debe ser responsabilidad de cada uno estar al tanto de para qué utilizaran los datos suministrados así como en el diario vivir se maneja con mucha cautela cualquier tipo de contraseña. En el caso de las empresas que manejan bases de datos, debe ser una obligación que se manejen y se cumplan reglas que tengan que ver con el manejo de la información personal de sus clientes y que estás se cumplan al pie de la letra.

En cuanto el momento en el que se autorizan la utilización de los datos, el cliente o usuario que brinde la información debe constatar y hacer cumplir el permiso que brindó para utilizar sus datos para el fin que inicialmente le indicaron. La empresa debe ser clara con la información del documento de autorización y explicar a dónde llegarán los datos, para qué se utilizarán y explicar, además, qué hacer en caso de que esto no se cumpla como una orientación a la cual el usuario tiene derecho.

Finalmente, se establece que la tecnología cada vez involucra más a todas las personas y una manera que se está utilizando para atraer clientes y para aprobar o rechazar créditos son las redes sociales, ya que, sin necesidad de tener cuentas oficiales, fotografías y datos personales se

filtran en las redes por medio de amigos y familiares que comparten información en común, lo que hace casi imposible no tener información en estas comunidades virtuales.

La necesidad de publicar y exponer sucesos de la vida que enorgullecen en un ejercicio de alarde a una "vida perfecta", lleva a que se comparta información que por seguridad debe permanecer en la vida privada de las personas, por ingenuidad y falta de conocimiento están en una constate entrega de información valiosa para quienes cometen delitos informáticos, siendo víctimas de violación de la intimidad, vulnerando su derecho al buen nombre y siendo afectados por chantajes y extorsiones.

Lo que implica también ser estrictos en cuanto a quienes se acepta como contacto en perfiles, partiendo que las redes sociales no se crearon para hacer amigos sino para acercarse más a ellos y más si se tiene en cuenta que según artículo 2° de la Ley de Hábeas Data, "esta solo se aplica al tratamiento de datos personales efectuado en territorio colombiano o en caso de que el responsable establecido en el exterior se rija por la legislación interna, en virtud de tratados internacionales" Superintendencia de Industria y Comercio (Superindustria).

Por lo tanto, las empresas aunque consigan la información por este medio se debe dar un buen manejo en la base de datos, teniendo en cuenta que sin una autorización previa no se puede realizar ningún procedimiento.

GLOSARIO

Para efectos de entender las políticas de tratamiento que se le debe dar a las bases de datos es importante explicar las siguientes definiciones que tienen relación con ley 1266 de 2008 en su artículo 3

- **Titular de la información:** El titular de la información es la persona natural o jurídica, quien suministrara unos datos que serán de gran importancia para empresas que buscan obtener clientes.
- **Fuente de información:** Es la persona, la entidad o la organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial, de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final.

  Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos. (Ley 1266 de 2008 articulo 3).
- Operador de información: Es la entidad o la organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley. Por tanto el operador, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la

protección de los derechos del titular de los datos.

- **Usuario:** Es la persona natural o jurídica que puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos. (Ley 1266 de 2008 articulo 3).
- **Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.
- **Base de Datos:** Conjunto organizado de datos personales que serán objeto de tratamiento por diversas empresas.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.
- **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o asociada con otros, decida sobre la base de datos o el manejo que se le dará a los datos.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

REFERENCIAS

Bergel, Salvador D. (2002). El hábeas data: instrumento protector de la privacidad.

Cifuentes Muñoz, E. (1997). El hábeas data en Colombia, en *Ius Et Praxis*, Chile, Universidad de Talca, Faculta de Ciencias Jurídicas y Sociales, 1997, pp. 85-87).

Congreso de la Republica. (31, 12, 2008). Ley Estatutaria 1266. Artículo 3. Disponible en https://www.bancoldex.com/documentos/1291_Ley_1266_de_2008_(Habeas_Data).pdf

Congreso de la Republica. (17, 10, 2012). Ley Estatutaria 1581. Artículo 10. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Constitución política de Colombia [Const.] (1991) Artículo 15 [Titulo II]. 2da Ed. Legis.

Constitución política de Colombia [Const.] (1991) Artículo 85 [Titulo II]. 2da Ed. Legis.

Corte Constitucional (25 de marzo de 2014). Sentencia T-176A/14

Corte Constitucional (16 de junio de 1992). Sentencia T-414 de 1992. Magistrado Ponente Ciro Angarita Barón

Corte Constitucional (1 de marzo de 1995). Sentencia 082-1995. Magistrado ponente Jorge Arango Mejía.

Corte Constitucional (17 de enero de 2001). Sentencia C- 748 de 2011.

Corte Constitucional (21 de junio de 2012). Sentencia 458 de 2012.

Remolina Angarita N. (2012). Tratamiento de datos personales, aproximación internacional y comentarios a la Ley 1581 de 2012.

Losano M. (1985) Informatica per le scienzesociali Giulio Einaudieditores.p.a

Ministerio de tecnologías y la información. Recuperado de http://www.mintic.gov.co/portal/604/w3-article-4425.html