REVISTA
CES DERECHO

Artículo de reflexión

Los datos personales y sus riesgos jurídicos a partir de la transformación digital en el comercio electrónico

Personal data and its legal risks from digital transformation in the electronic commerce

Deisy Yolima Niño García [1] ✉

[1] Abogada de la Universidad Libre, Especialista en Derecho Comercial y Magíster en Derecho con énfasis en Derecho Privado de la Universidad del Rosario.

Fecha correspondencia:
Recibido: septiembre 10 de 2021.
Revisado: enero 20 de 2022.
Aceptado: enero 24 de 2022.

Forma de citar:
Niño, Deisy Yolima." Los datos personales y sus riesgos jurídicos a partir de la transformación digital en el comercio electrónico" En: Revista CES Derecho. Vol. 13, No. 1, enero a abril de 2022, p. 70-89. https://dx.doi.org/10.21615/cesder.6386

Open access
© Derecho de autor
Licencia creative commons
Ética de publicaciones
Revisión por pares
Gestión por Open Journal System
DOI: 10.21615/cesder.6386
ISSNe 2145-7719

Publica con nosotros

Resumen

Este artículo se enfoca en los riesgos jurídicos que se presentan al momento de suministrar los datos personales o sensibles a las diferentes plataformas digitales, en el comercio electrónico, en las redes sociales y las entidades financieras. Se busca concientizar a personas naturales y jurídicas sobre los riesgos, así como sus derechos y deberes, mencionando además las responsabilidades de las empresas en el cuidado y la protección de los datos personales.

Se llevó a cabo una revisión de las sentencias de la Superintendencia de Industria y Comercio (SIC), y las guías sobre el tratamiento de datos personales elaboradas por la delegatura de protección de datos personales.

Se concluye que, si bien las personas autorizan el uso de los mismos, las compañías tienen la responsabilidad de protegerlos ya que se pueden generar daños económicos, sociales e incluso reputacionales.

Palabras clave: comercio electrónico; datos personales; riesgos jurídicos; SIC; consumidores.

Abstract

This article focuses on the legal risks that arise when supplying personal or sensitive data in the different digital platforms, in e-commerce, in social networks and financial entities. It seeks to make natural and legal persons aware of the risks, as well as their rights and duties, also mentioning the responsibilities of companies in the care and protection of personal data.

A review was carried out of the judgments of the Superintendence of Industry and Commerce (SIC), and the guides on the processing of personal data elaborated by the delegation of protection of personal data.

It is concluded that, although people authorize their use, companies have the responsibility to protect them since economic, social and even reputational damage can be generated.

Keywords: electronic commerce; personal data; legal risks; SIC; consumers.

Introducción

Muchas veces nos preguntamos ¿qué son los datos personales y para qué sirven? y ¿Cuál es la importancia de protegerlos?, algunas veces no se nos brinda información suficiente acerca de lo sensible y delicado que puede ser su manejo.

La Superintendencia de Industria y Comercio (de ahora en adelante la SIC) nos indica lo siguiente en la guía de protección de datos personales:

Cuando hablamos de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos (Superintendencia de Industria y Comercio, 2021b, párr. 2).

Para recopilar los datos personales las compañías deben de contar previamente con una autorización por parte del titular de los datos, quien debe tener conocimiento para que y como se utilizará dicha información. Para que esto se pueda hacer, “la organización responsable del tratamiento de los datos debe adoptar procedimientos internos para solicitar la autorización al titular” (Superintendencia de Industria y Comercio, s. f., p. 7).

Estos datos son entregados en muchas ocasiones, cuando vamos hacer alguna compra, solicitar una cita médica, ingresar a un establecimiento en el que, por temas de bioseguridad con el Covid-19, debemos suministrar nuestros datos; cuando queremos descargar una aplicación en nuestro celular o ingresar a una página web (algunas de las cuales no son muy seguras), cuando

se está en búsqueda de una oportunidad laboral, entre otras. Proporcionamos esta información a infinidad de plataformas y/o empresas que la solicitan. En fin, si nos ponemos a pensar, muchas veces estamos entregando información sin ver más allá de las consecuencias.

Analicemos un caso que no sea solo para adquirir un producto o servicio a través de un medio electrónico, si no cuando una persona quiere ingresar a un edificio pero, para que sea autorizado su ingreso este debe entregar sus datos como: el nombre, el número de cédula, el teléfono y a su vez, le toman una foto y le solicitan su huella, ¿qué pasa si esta persona se rehúsa a entregar la información solicitada? no podrá ingresar al edificio, y si no tiene más opción que entregarlos, por una cita o reunión importante, esta persona finalmente confía en que el sujeto que le está tomando los datos personales o el administrador del edificio no van hacer un mal uso de estos. Puede que el edificio cumpla con los procedimientos establecidos en la Ley 1581 de 2012, y se tenga todos los documentos en regla, pero, ¿cómo puede el administrador del edificio tener la certeza de que la persona que toma los datos no va hacer un mal uso?, o ¿cómo puede la ley castigar al administrador del edificio, en caso de que se presenten irregularidades en el tratamiento de los datos personales?.

Entre la persona que ofrece los datos y la persona que los recopila como el administrador del edificio deben establecer una relación de confianza, y garantizar que se están siguiendo todos los requisitos legales. La confianza radica en que nuestros datos van a ser debidamente protegidos, pues se han entregado por un consentimiento libre con la finalidad de que estos no sean divulgados. Es importante resaltar que para los habitantes de este edificio es fundamental la recopilación de los datos de quienes entran al edificio, para así tener la confianza de que nadie extraño o mal intencionado pueda interrumpir la seguridad del edificio.

Ahora bien, este tipo de ejemplo es muy similar cuando se entregan los datos a través del comercio electrónico para obtener un bien o servicio, pues si no se suministran, no se podrá adquirir lo que se necesita. Así como el administrador del edificio, la empresa a la que le entregamos los datos tiene el deber de protegerlos.

Adicional a estas situaciones, algunas plataformas solicitan información que no es relevante o acorde para lo que se autoriza el uso de los datos personales, como sucede, cuando se está en busca de una oportunidad laboral y se aplica en diferentes plataformas ya sea porque se adjunta la hoja de vida con información personal, o porque se ingresan los datos en un formulario pre-diseñado por la compañía, por ejemplo, cuando solicitan información que no es relevante para el cargo al que se aspira, pero la necesidad que se tiene de obtener un trabajo se suministran esos datos, sin pensar más allá de cómo estos pueden estar siendo manipulados. Se debe crear consciencia que los datos personales hacen parte de la intimidad de las personas y que están ligados a un derecho fundamental.

La Corte Constitucional en sentencia T-610/2019 (2019) ha manifestado que hay cinco principios que certifican la importancia frente al derecho de la intimidad, los cuales son:

> (i) el principio de libertad, que predica que el registro o divulgación de los datos personales requiere de su consentimiento libre, previo, expreso o tácito, o que exista una obligación de revelar dicha información con el fin de cumplir un objetivo constitucionalmente legítimo;
>
> (ii) el principio de finalidad, el cual demanda "*la exigencia de someter la recopilación y divulgación de datos, a la realización de una finalidad constitucionalmente legítima*";
>
> (iii) el principio de necesidad, de acuerdo con el cual la información personal divulgada guarde "*relación de conexidad con la finalidad pretendida mediante su revelación*";
>
> (iv) el principio de veracidad, el cual exige que los datos personales que puedan ser divulgados "*correspondan a situaciones reales*" y, por último,
>
> (v) el principio de integridad, según el cual, la información que sea objeto de divulgación debe suministrarse de manera completa, impidiendo que se registre y presente datos parciales, incompletos o fraccionados (p. 16).

El derecho a la intimidad se entiende como el circulo que protege la vida privada de las personas, frente a situaciones ajenas, mediante la protección que otorga la ley (López Jiménez, 2011). Hacer un uso adecuado y confiable de los datos es la esencia de la protección de la persona, ya sea natural o jurídica. Por un lado, las personas naturales deben preguntarse ¿qué información ofrecen?,¿a quién? y si esta es protegida. Por otro lado, para las empresas, el almacenamiento y el cuidado de esta información trae consigo responsabilidades jurídicas y éticas; a pesar que estos datos le puedan traer un valor "agregado", al incrementar su base de datos para, a futuro, poder realizar mercadeo y ventas entre sus clientes.

Para el desarrollo del presente artículo, se analizarán los canales digitales en los que comúnmente las personas entregan sus datos personales, así como los riesgos jurídicos que pueden llegar a presentarse. Dentro de los cuales tenemos: el comercio electrónico, las redes sociales y los medios virtuales de las entidades financieras. Más adelante, se analizan los derechos que tienen los titulares de los datos personales; y finalmente, quienes serían los responsables de proteger los datos personales.

Tratamiento de datos personales en el comercio electrónico

La transformación digital y la pandemia dada por el Covid-19 aceleraron e incrementaron el uso del comercio electrónico *(e-commerce).* Las personas se han visto favorecidas, dado que lograron satisfacer diferentes necesidades, a pesar de no acceder físicamente a los diferentes

establecimientos comerciales. Por un lado, el comercio electrónico generó la facilidad de realizar compras desde cualquier lugar del mundo, sin la necesidad de medir fronteras; por otro lado, les ahorró tiempo a las personas, ya que ahora no tienen que pasar horas en el tráfico o haciendo una fila para poder realizar un pago. Estos beneficios han venido cambiando el comportamiento de los seres humanos, debido a que han transformado la forma de comunicarse, trabajar, hacer negocios, mantenerse informado e incluso divertirse. Cada vez son más las compañías que usan este canal para entablar una conexión y experiencia digital con sus clientes, enfocado a satisfacer sus necesidades frente la adquisición de algún producto o servicio.

De acuerdo con la Ley 1480 de 2011 en su artículo 49, el Comercio Electrónico es: "la realización de actos, negocios u operaciones mercantiles concertados a través del intercambio de mensajes de datos telemáticamente, cursados entre proveedores y los consumidores para la comercialización de productos o servicios" (Congreso de la República de Colombia, 2011). Además, de acuerdo con el artículo 2 literal b de la Ley 527 de 1999 se crea una relación contractual, entre la compañía y el consumidor, "cuestiones suscitadas por toda la relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro similar" (Congreso de la República de Colombia, 1999).

Sin duda, el crecimiento que ha tenido el *e-commerce* a través de los años ha sido de gran importancia, según la SIC "El comercio electrónico es el motor de la economía del siglo XXI y los datos personales es la moneda de la economía digital" (Superintendencia de Industria y Comercio: Delegatura para la protección de datos personales, 2019, p. 1). Las actividades que abarca el *e-commerce* implican la recolección de los datos personales de los consumidores al momento de hacer cualquier tipo de transacción, y con esta solicitud se inicia una relación de confianza entre el consumidor y el proveedor del servicio. Para recopilar los datos personales, las empresas deben contar con una autorización por parte del titular de los datos; esta puede ser por escrito, de manera oral, o mediante evidencias: videos donde se captura la autorización del titular. Sin importar por cual vía se otorgue la autorización se debe conservar prueba de ello (Superintendencia de Industria y Comercio, s/f-a, p. 8).

Al momento de realizar una compra, solicitar un servicio por internet, descargar una aplicación, los consumidores deben inscribir y registrar sus datos personales en una plataforma digital, y con esto las compañías almacenan la información en su base de datos y generan un valor adicional. Los datos que solicitan son el nombre, la cedula, la dirección, el teléfono, los números de la tarjeta de crédito y su clave. Estos aspectos solo son de conocimiento del consumidor que entregan de buena fe a estas plataformas digitales, por esta razón deben ser protegidos, tanto en su tenencia como en su tratamiento por los terceros autorizados (López Jiménez, 2011). Cuando hablamos de valor adicional se hace referencia a la posibilidad que tienen las compañías de generar un acercamiento asertivo hacia el consumidor, dado que conocen nuestros intereses y necesidades, lo cual puede generar un incremento en sus ventas. Por

ejemplo, cuando llega publicidad al celular, al correo electrónico, etc., acerca de un producto que consumes regularmente con descuentos especiales. En este caso las compañías crean unos perfiles con el fin de capturar la atención del consumidor y que este crea la necesidad de compra.

Estos datos, al ser de carácter privado, pueden llegar a ser susceptibles, el no tener el manejo adecuado de ellos puede traer consigo grandes riesgos como suplantación de identidad, robo, fraude, entre otros delitos. 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.

A continuación, se procederá a explicar cuáles son los posibles riesgos jurídicos que se pueden llegar a presentar en el comercio electrónico y como pueden llegar a ser capturados nuestros datos por terceros no autorizados en las diferentes plataformas digitales.

Posibles riesgos jurídicos

Un año después del Covid-19, una investigación por parte de TransUnion muestra que el 30% de los consumidores colombianos han sido blanco de fraude digital. El estudio se hace analizando 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).

De acuerdo con el artículo de TransUnion [1] (2021) Manuel Piñeros, dice:

> Los estafadores siempre buscan aprovecharse de eventos mundiales significativos y la pandemia ha sido un acelerador digital para empresas y personas que también ha conllevado un riesgo en materia de delincuencia en línea. (párr. 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.

Es necesario, comprender que significa la suplantación, para esto la guía sobre el tratamiento de datos personales para fines de Comercio Electrónico, la define como:

[1] Es una central de riesgo que ayuda a las empresas a tomar decisiones de negocio como por ejemplo la aprobación de crédito a los bancos de acuerdo a la historia crediticia y cupo de las personas.

> Suplantar significa, entre otras, "sustituir ilegalmente a una persona u ocupar su lugar para obtener algún beneficio". La suplantación de identidad consiste en hacerse pasar por otra persona para diversos propósitos: engañar a terceros, obtener bienes y servicios con cargo a la persona suplantada, incurrir en fraudes y otros tipos de conductas ilícitas. (Superintendencia de Industria y Comercio: Delegatura para la protección de datos personales, 2019, p. 9).

La suplantación de identidad se puede llegar a presentar en diferentes situaciones en el *e-commerce,* pero, ¿Cómo pueden los delincuentes obtener los datos personales? existen casos, en los cuales, los delincuentes ingresan al sitio web o el *e-commerce* del banco con el usuario y contraseña de la víctima, la cual, obtienen por diferentes formas, una de ellas es por medio de inteligencia social, por ejemplo, empiezan a contactar a la víctima ya sea por medio de correos electrónicos o mensaje de texto al celular (datos que son personales) y le dicen a la víctima que su cuenta bancaria tuvo un intento de fraude, lo cual no es cierto, y para evitar el fraude se le solicita que por favor actualice sus datos personales, la persona por miedo al supuesto fraude accede colocando sus datos en un formulario falso y con esa encuesta los delincuentes obtienen la información del cliente.

Un segundo método, más sofisticado 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. Al momento de que el consumidor entra a su banco para hacer alguna transacción, el software captura la información del cliente sin que este se percate de lo que está sucediendo.

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.

Adicional a ello, se roban la línea del cliente, para que al momento en que los delincuentes estén suplantando al cliente real y estén realizando la transacción, el banco les envié un pin al número de celular para "verificar" que la transacción es real, pasando así el defraudador un filtro de seguridad realizando robos en las diferentes cuentas bancarias.

[2] Existen muchos tipos de malware, como los virus informáticos, los troyanos, los gusanos, el spyware, el adware y el ransomware. Sin embargo, malware es el término principal que se utiliza para hablar de todas esas amenazas informáticas.

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: Delegatura para la protección de datos personales, 2019).

Otra situación, que se presenta a menudo es cuando le llega información al consumidor para venderle algún servicio o llaman de entidades bancarias para ofrecer algún tipo de producto del cual no se ha tenido ninguna relación, y nos preguntamos ¿cómo pueden llegar a obtener nuestro número de teléfono o correo electrónico? para que nos llegue esta información, las hipótesis pueden ser muchas y entre esas es que algunas personas se encargan de manera poco responsable de obtener este tipo de información y ponerla a servicio de entidades o empresas que la requieran para así poder tener un mayor número consumidores y generar más ventas. Por seguridad se puede solicitar a la entidad que brinde información de donde saco los datos personales y que estos sean eliminados.

Los datos personales se obtienen cuando los autorizamos para su tratamiento, pero algunas veces estos se filtran y llegan a manos de terceros no autorizados para manipularlos o consultarlos de manera fraudulenta. También hay casos en los cuales, las personas publican en sus redes sociales datos e información que puede ser sensible.

Datos personales en las redes sociales

La era digital no conoce fronteras, con las redes sociales estamos dando acceso de una manera muy amplia a nuestra información y privacidad, tanto a conocidos como a desconocidos, por ejemplo, en la red social Facebook, con aproximadamente 2.410 millones de usuarios en todo el mundo (Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio, 2019a) circula, además de nuestra información personal, nuestras creencias políticas, religiosas, sociales, etc., intereses, necesidades entre otros aspectos, dejándonos expuestos y vulnerables ante los otros.

Por medio de estas redes se da a conocer datos sensibles de las personas, los cuales, la SIC en la guía de protección de datos personales, los define de la siguiente manera:

> Son 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 garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos (Superintendencia de Industria y Comercio, 2021c).

Las redes sociales es una plataforma donde las personas haciendo uso de su libertad de expresión manifiestan de manera abierta y expontanea su ideología politica o inclinación sexual, entre otros. Algunas veces pueden llegar a sufrir de descriminación y/o ataques por partes de terceros que no comparten sus pensamientos por causa de estas preferencias o ideologías. Existen otro tipo de riesgos, en cuanto a la cantidad de engaños que se pueden generar por medio de las redes sociales, por ejemplo, se pueden crear perfiles falsos con las fotos publicadas por las personas, por medio de los cuales suplantan la identidad para generar diferentes tipos de delitos, lo cual afecta el buen nombre, es decir, la reputación o el concepto que se tiene de una persona.

Ante este tipo de situaciones se deben tener medidas de seguridad para no poner "[…] en riesgo algunos derechos humanos y convierten el tratamiento de datos personales en una actividad indebida e inconsistente con los mandatos constitucionales y legales" (Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio, 2019a, p. 1). Por consiguiente, las compañías por medio de las cuales los usuarios utilizan para expresarse libremente o simplemente compartir sus fotos o vida diaria deben proporcionar "garantía del habeas data y del derecho a la intimidad, y además se encuentra estrechamente relacionada con la protección de la dignidad humana"(Corte Constitucional, 2011, p. 203).

Cuando se presentan este tipo de situaciones en las redes sociales se debe de proteger los derechos de las personas vulneradas, para esto, el responsable del tratamiento de los datos personales debe tomar medidas acordes, protegiendo la información del perfil del usuario mediante "parametros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos"(Corte Constitucional, 2011, p. 197) permitiendo así los estandares de protección consagrados en la Ley.

Si bien, las redes sociales traspasan las fronteras y nuestros datos circulan a través de internet de una manera difícil de controlar, esto no significa que no se tenga la obligación de cumplir con las normas, sobre todo porque se debe de proteger y respetar los derechos fundamentales, como es el derecho a la intimidad.

> La Corte Constitucional ha precisado que "en internet, (…) puede haber una realidad virtual, pero ello no significa que los derechos, en dicho contexto, también lo sean. Por el contrario, no son virtuales: se trata de garantías expresas por cuyo goce efectivo en el llamado ciberespacio" también debe velar el juez constitucional". Recalca dicha

> corporación que “nadie podría sostener que, por tratarse de Internet, los usuarios si pueden sufrir mengua en sus derechos constitucionales” (Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio, 2019a, p. 2).

En ese sentido, por la cantidad de información que se recolecta en las redes sociales, las compañías deben reforzar sus medidas de seguridad, pues no podemos olvidar que la información tanto personal como sensible que se maneja en estas redes es muy amplia, la cual puede traspasar fronteras, y “el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre (Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio, 2019c, p. 4).

Aun cuando usemos las redes sociales para compartir nuestras ideologías o nuestra vida privada, debemos ser conscientes que tenemos derechos, los cuales podemos exigir en el momento en que consideremos que los mismos se encuentran vulnerados. Pero también debemos generar una consciencia y ser prudentes de lo que compartimos en estas redes, pues si bien existe el derecho a la libre expresión, esto no quiere decir que no debamos de ser más preventivos.

El uso de datos personales en entidades financieras

Sin duda alguna, uno de los entes que más recopila y guarda información privada de las personas son las entidades bancarias, desde el momento que una persona natural o jurídica abre una cuenta de ahorros o corriente suministra todos los datos personales, así como el libre acceso a los estados financieros.

Las entidades bancarias, como cualquier otra compañía que requiera la recolección de datos, debe contar con una autorización por parte del titular que provee la información, la cual debe ser previa, libre. De no ser así, las entidades estaría violando el principio de libertad que tienen los titulares (Superintendencia de Industria y Comercio, 2021a).

Como se indicó anteriormente, las entidades financieras tienen acceso a nuestros datos, pero existen riesgos en los cuales:

> Si un dato personal es conocido, accedido o sustraído por terceros no autorizados, por ejemplo, piratas cibernéticos, esta situación entraña per ser un riesgo para los derechos y libertades de los individuos, de gravedad y probabilidad variables (Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio, 2019c, p. 6).

Es decir, cuando hay una suplantación de identidad, fraude, o daños económicos, se puede llegar a presentar porque terceros mal intencionados abren cuentas bancarias a nombre de otra persona, lo cual desencadenaría en “daño al buen nombre, pérdida de confidencialidad o

cualquier otro perjuicio económico o social significativo para los individuos" (Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio, 2019c, pp. 6 y 7). Existen otros casos, donde los usuarios han sufrido de suplantación cuando les han sustraído dinero de sus cuentas bancarias o tarjetas de crédito generando con ello no solo un perjuicio económico para la persona sino también para el banco, ya que al descubrir el fraude y corroborar la identidad de la persona es el banco quien asume está perdida. Cuando el uso de datos responde a unos intereses particulares; el cliente puede sufrir doble carga, por un lado, ser víctima de un delito, y, por otro lado, demostrar que no fue quien llevo a cabo la infracción de la ley.

Situaciones como la anterior, pueden llegar a ser bastante recurrentes cuando se tiene acceso a los datos personales de manera irregular. Para evitar inconvenientes o posibles fraudes, los bancos deben trabajar en controles y medidas de prevención, a través de sus *e-commerce*, los cuales se pueden dar en diferentes etapas del proceso: (i) cuando el cliente abre una cuenta ya sea de ahorros o corriente, (ii) cuando el cliente ingresa al *e-commerce* para realizar sus consultas bancarias, e incluso al momento de ejecutar una transacción bancaria como es al realizar un pago, (iii) al realizar una transferencia electrónica, situaciones donde el banco debe tener una mayor seguridad.

Es importante que exista una estructura de seguridad informática muy robusta en cuanto a la infraestructura, conectividad, redes, y acceso de las diferentes plataformas y servidores del banco, como también a las terminales o computadores personales desde donde accede el personal, políticas de seguridad informática que proteja la información al momento que un tercero entre y acceda a la red interna del banco y así, sustraiga información de los usuarios y pueda con esta generar grandes estafas tanto para el banco como para los clientes.

A su vez, las entidades financieras deben ejercer capacitaciones, campañas de concientización entre los colaboradores acerca de la importancia y cuidado de los datos, no solamente en los procesos a los que se deben de regir, también al conocimiento y control de los mismos. Además, sería pertinente que las entidades elaboren campañas de publicidad en donde le indiquen al cliente la necesidad de exigir la protección de sus datos personales. A esta campaña informativa se debe involucrar a terceros, como: los analistas de atención de servicio al cliente, las casas de cobranza y proveedores que hacen parte de todo el ecosistema bancario.

No obstante, algunas entidades bancarias manejan un esquema de seguridad cuando el cliente ingresa a su *e-commerce*, aparte de digitar el usuario y la contraseña debe ingresar un código de seguridad que puede ser enviado al correo electrónico, o mediante mensaje de texto al celular. Esto se hace con el fin de verificar que realmente la persona que va a ingresar a la plataforma sea el titular de la cuenta y no un tercero no autorizado.

Hay entidades bancarias que tienen información de personas que nunca les han proporcionado autorización para el manejo de sus datos, y aun así utilizan los datos para fines comerciales, lo que demuestra que en algunas situaciones no tienen un adecuado manejo en el uso de los datos.

En otro orden de ideas, es importante que las personas tanto naturales como jurídicas conozcan la importancia de los datos personales, cuales riesgos se pueden llegar a presentar, y cómo se puede llegar a evitar situaciones incomodas que generen algún perjuicio moral o económico.

Derechos de los titulares de los datos personales

Todo ciudadano tiene el deber de conocer sus derechos legales frente al uso de los datos personales, en muchas ocasiones estos se proporcionan sin tener clara la importancia de los mismos, y solo se entregan por la necesidad de hacer una compra o adquirir algún servicio. Debemos aprender a hacer uso de nuestros derechos, para así crear un sistema más cooperativo y proteger los datos, que son un intangible muy valioso.

Ante cualquier situación, es importante que el lector tenga pleno conocimiento de que las compañías dueñas del *e-commerce* deben contar con un requisito indispensable, que es la autorización previa, expresa e informada por parte del titular, para que sus datos ingresen a la base de datos y se utilicen para los fines autorizados (Superintendencia de Industria y Comercio, s/f-a). Por ejemplo, si los datos son solicitados en el momento de realizar una compra mas no para que la compañía envíe información de promociones, estos no pueden ser utilizados para lo último.

Los datos se puedan actualizar, incluso rectificar, en caso de que la persona haya cambiado de domicilio o número telefónico. Así mismo, se tiene el derecho de revocar esta autorización o solicitar que los datos sean eliminados (Congreso de la República de Colombia, 2012). En cualquiera de los casos el consumidor no tiene por qué brindar ningún tipo de explicación: es suficiente con la voluntad de realizar el trámite que considere pertinente.

Siguiendo la línea de lo anteriormente mencionado, la Corte Constitucional ha definido el derecho de *habeas data* en los siguientes términos:

> El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos conforme a los principios que informan el proceso de administración de bases de datos personales. (Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio, 2019b, p. 4).

Para tener un poco más de claridad, podemos analizar el siguiente caso, que se presenta cuando las entidades bancarias realizan alianzas con diferentes compañías de telecomunicaciones [3], y comparten los datos personales de los usuarios para obtener un amplio portafolio de clientes y ofrecer sus productos, como tarjetas de crédito, o para ofrecer atractivas tasas de interés para compra de cartera, entre otros. Aunque las entidades bancarias realicen este tipo de alianzas, deben contar previamente con una autorización expresa por parte del titular de los datos personales, pues se debe conocer cuál será el uso de los datos. En el presente caso, el titular de los datos solo autorizó a la empresa de telecomunicaciones a usarlos en virtud de la relación contractual que tenía con esta, mas no para que los compartiera con empresas aliadas. Cuando la entidad financiera llamó al cliente para ofrecer sus productos, este solicitó que sus datos fueran eliminados de la base de datos, pues no le interesaba adquirir ningún tipo de producto. Ninguna compañía puede usar, para sus fines comerciales, los datos personales de una manera deliberada y no autorizada, ya que esto puede generar graves sanciones por parte de la SIC.

Es importante que los consumidores tengan en cuenta que las compañías responsables deben poner a disposición del "titular mecanismos gratuitos y de fácil acceso para poder presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada" (Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio, 2019b, p. 7). En caso de alguna inconformidad o para poder hacer valer sus derechos, los consumidores deben, en primer lugar, presentar una queja ante la compañía. En caso de que la respuesta no sea favorable o que dentro de los quince (15) días de haber instaurado la queja no se tiene respuesta, podrán presentar una queja formal ante la SIC, quien, como entidad encargada de proteger los datos personales, llevará a cabo la correspondiente investigación (Superintendencia de Industria y Comercio, s/f-c, p. 10).

El titular de los datos personales tiene derechos, pero no siempre es consciente de ellos, razón por la cual es necesario crear consciencia sobre la importancia de los mismos. El consumidor debe ser prudente a la hora de compartir información personal o sensible, pues mucha de esta información puede ser utilizada para fines distintos a los anunciados. Aunque nuestra legislación es proteccionista y las compañías tienen deberes, no debemos olvidar que hay terceros que se aprovechan de esta información, generando riesgos jurídicos como los ya mencionados en el desarrollo del presente artículo.

Responsabilidad en la protección de los datos personales

Para los consumidores y las compañías "es importante tener presente que ni la Constitución ni la Ley se oponen al tratamiento de datos personales para fines de comercio electrónico. Las dos solo exigen el cumplimiento de unas garantías mínimas" (Superintendencia de Industria y

[3] Caso tomado de la Resolución 10720 de 2020, proceso adelantado contra el Scotiabank Colpatria S.A en una alianza realizada con la empresa de telecomunicaciones de ETB, en la cual, el banco Colpatria no contaba con autorización por parte del titular de los datos personales, por ende, la SIC sanciono al banco por el uso indebido de los datos personales del titular.

Comercio: Delegatura para la protección de datos personales, 2019, p. 2). Sin embargo, se debe tener claro sobre quién recae la responsabilidad de este manejo, pues si bien las personas de buena fe entregan sus datos, las compañías tienen la obligación de contar con el equipo necesario para su propia protección ante terceros que sustraigan la información de manera irregular. Las compañías "son meros tenedores que están en el deber de administrar de manera correcta, apropiada y acertada la información de las personas porque su negligencia afecta los derechos humanos de los titulares de los datos" (Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio, 2021, p. 12).

A nivel nacional, la Superintendencia de Industria y Comercio desempeña una labor muy importante, ya que es la entidad que se encarga de ejercer el control para que las compañías lleven a cabo, de una manera segura, este proceso, así como la de imponer las respectivas sanciones. Por medio de la SIC y de acuerdo con la Ley 1581 de 2012, se regula el tratamiento de los datos personales, los derechos y obligaciones que se adquieren por un vínculo contractual que se genera entre las compañías y los consumidores, en el momento de realizar cualquier tipo de transacción. A nivel de organismos internacionales también se presentan propuestas para la protección del consumidor en el comercio electrónico.

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha recomendado lo siguiente sobre privacidad y seguridad:

> 48) las empresas deberían proteger los datos personales del consumidor, asegurándose de que sus prácticas relacionadas con la recopilación y el uso de datos del consumidor sean legales, transparentes y justas, y que permitan la participación y elección del consumidor y tomen precauciones de seguridad razonables.
>
> 49) Las empresas deberían de gestionar el riesgo relacionado con la seguridad digital e implementar medidas de seguridad para reducir o mitigar los efectos adversos relacionados con la participación del consumidor en el comercio electrónico (Superintendencia de Industria y Comercio: Delegatura para la protección de datos personales, 2019, p. 1).

La SIC considera importante que es deber de las compañías asegurarse que quien suministra los datos sea realmente quien dice ser y no un suplantador de identidad. Para ello sugiere que los procesos implementados puedan responder a los siguientes interrogantes: ¿Cómo tener certeza de que una persona es quien dice ser? La certeza se puede obtener con validación biométrica o con consultas de información a entidades que tengan información confiable, como las centrales de riesgos. ¿Cómo identificar electrónicamente a la persona? ¿Cómo impedir suplantaciones físicas o electrónicas? ¿Cómo verificar quién envió un mensaje de datos o expresó su voluntad? (Gutiérrez & Cure, 2020, párr. 6).

Existen diferentes métodos para verificar una suplantación, para esto las compañías deben de invertir en recursos que les permita corroborar la información ya sea esta por medio de biometría dactilar, facial, o del iris, así, como validar la información biométrica del cliente y compararla con entidades certificadas con la Registraduria Nacional del Estado Civil, para así verificar en tiempo real si se trata de la persona o no, por ejemplo, las entidades de telecomunicaciones como Movistar usan biometría dactilar con conexión a la Registraduria Nacional del Estado Civil, o, cuando se ingresa al país al momento de realizar migración hay un proceso de verificación del iris. Esos procesos permiten validar la identidad de la persona sea quien dice ser.

Con base a lo anterior, y teniendo en cuenta que las empresas son las responsables de proteger los datos personales, la SIC en su calidad de autoridad en la protección de datos personales creo la guía para la implementación del principio de responsabilidad demostrada (*Accountability*), la cual, pretende orientar a las compañías para que lleven a cabo una estructura interna y así puedan tener un personal calificado para adelantar procedimientos completos y asertivos.

De manera concreta, el artículo 27 del Decreto 1377 de 2013 exige que esas políticas garanticen:

> (i) La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la ley.
>
> (ii) La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación, y
>
> (iii) La adopción de procesos para la atención y respuestas a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del Tratamiento (Superintendencia de Industria y Comercio, s/f-b, p. 9).

El principio de seguridad que indica la Resolución 21478 de 2019, exige lo siguiente:

> Que la información esté sujeta a Tratamiento se maneje con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a esos registros evitando adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Esto significa que, por regla general todas las organizaciones que tratan datos personales deben contar con mecanismos de seguridad robustos, sea dentro de la organización y cuando o a través de proveedores de servicios externos con la experiencia adecuada. Esto debe concluir mecanismos para: identificar con precisión y rapidez las vulnerabilidades que necesitan corrección; implementar las correcciones adecuadas para que las

> vulnerabilidades que se presenten se corrijan de forma expedita; y verificar que las vulnerabilidades hayan sido corregidas (Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio, 2019c, p. 3).

Es importante tener en cuenta, que estas medidas no deben estar condicionadas a que el consumidor presente algún daño o perjuicio por entregar sus datos personales, el hecho de que el titular de los datos lo suministre es suficiente para que las compañías lleven a cabo las medidas necesarias para prevenir cualquier riesgo (Ministerio de Comercio, Industria y Turismo Superintendencia de Industria y Comercio, 2019c, p. 35).

Por otro lado, los usuarios cuando sufren alguna afectación ya sea económica o a su buen nombre tienen que hacer uso de los entes de control para obtener una solución ante una vulneración de sus derechos y más si se trata de los datos personales, pero esto no debería de ser así, las compañías dueñas del *e-commerce* deben ser más proactivos y preventivos ante cualquier tipo de riesgo que se presente ante la fuga de información de cualquiera de sus afiliados que pueda generar fraude, suplantación o robo de identidad, incluso abuso de confianza. La idea es que estos casos no lleguen a la SIC o a las diferentes autoridades de control si no que puedan evitarse antes de que un defraudador lo haga primero.

Se hace necesario tener mecanismos jurídicos no solo para cuidar a los usuarios que usan las plataformas de *e-commerce* sino de blindar a las compañías mediante procesos, controles y procedimientos internos para mitigar estos riesgos. También es importante desarrollar campañas periódicas y capacitación a los consumidores y a los colaboradores de las compañías para no caer en los engaños de los delincuentes informáticos, todo en un marco legal claramente definido, establecido y soportado en la Ley.

Conclusiones

Según lo planteado en el desarrollo del presente artículo, se permite analizar los posibles riesgos que se pueden llevar a cabo al momento de suministrar nuestros datos personales y la responsabilidad que tienen las compañías para protegerlos. Pero también se quiere dar a conocer al lector que tiene derechos como titular de los datos personales, entre los cuales se encuentran el conocer la información, actualizar, rectificar y eliminar la información que no ha sido autorizada (Superintendencia de Industria y Comercio, s/f-c, p. 8), así como de presentar la respectivas denuncias ante la Superintendencia de Industria y Comercio.

Los delitos informáticos han sido muy difíciles de identificar, así como llegar a judicializar a los responsables; en Colombia por ejemplo las autoridades llegan a un muy pequeño porcentaje de judicialización por la complejidad que supone el mundo informático en dónde los delincuentes se camuflan en las redes de información haciéndose pasar incluso por otras personas mediante la suplantación de identidad.

Por otro lado, es fundamental que el gobierno siga actualizando y creando políticas públicas para la protección de datos y un marco legislativo para combatir el Cibercrimen que afecta a los usuarios, instituciones y organizaciones del sector privado, dado que, si las compañías se blindan para evitar los posibles riesgos jurídicos se reducirían los diferentes fraudes.

Sin duda cada día la tecnología avanza a pasos agigantados, sabemos que esta no es una tarea fácil, aunque se trate de abarcar la mayor protección posible tanto para el consumidor como para las compañías, en algunos casos se pueden presentar espacios en el *e-commerce* que causen una debilidad ya que los defraudadores tratan de ir un paso adelante buscando las vulnerabilidades sin ser detectados. Al tratarse de información tan delicada nunca se sabe dónde pueda haber una fuga, incluso mientras una ley puede llegar a ser aprobada esta podría estar un paso atrás con los avances que se van dando en la era digital, con mayor razón todas las personas sin excepción debemos aprender y conocer la manera para ser más cuidadosos.

Es importante tener en cuenta que el manejo y cuidado de los datos personales, no es solo para evitar reclamos de los clientes defraudados, estafados o las posibles sanciones por parte de la Superintendencia de Industria y Comercio (SIC), sino sobre todo por el daño económico, social y reputacional tanto para la compañía dueña del *e-commerce* como para el consumidor que entrega sus datos confiando que estos estarán seguros y protegidos.

De tal forma, es muy significativo que las compañías que ofrecen el *e-commerce* como canal de ventas o atención de clientes tengan todas las condiciones jurídicas y mecanismos necesarios para prevenir estos fraudes y delitos informáticos. Sin duda, un cliente que se sienta seguro en una plataforma digital volverá a comprar en este sitio y se genera una relación de confianza. Igualmente, esta confianza con el usuario puede crecer mediante el desarrollo de plataformas con lineamientos establecidos de seguridad digital que les permitirán a los consumidores sentirse tranquilos a la hora de hacer sus transacciones comerciales.

Referencias

Congreso de la República de Colombia. (1999). Ley 0527 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial No. 43.673. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Congreso de la República de Colombia. (2011). Ley 1480 de 2011: Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones. Diario Oficial No. 48.220. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1480_2011_pr001.html#49

Congreso de la República de Colombia. (2012). Ley Estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial 48587. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Corte Constitucional. (2011, octubre 6). Sentencia C-748-11 M.P. Jorge Ignacio Pretelt Chaljub. Recuperado de https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

Corte Constitucional. (2019, diciembre 12). Sentencia T-610-19 M.S. Reyes Cuartas José Fernando. Recuperado de https://www.corteconstitucional.gov.co/relatoria/2019/T-610-19.htm

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. 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/

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/default/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: https://www.sic.gov.co/manejo-de-informacion-personal

Superintendencia de Industria y Comercio. (2021b). Protección de datos personales. 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 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: https://noticias.transunion.co/206-aumentaron-intentos-de-fraude-digital-originados-desde-colombia/