UNIVERSIDAD DEL ROSARIO

FACULTAD DE JURISPRUDENCIA

EL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA EN EL TRATAMIENTO DE DATOS PERSONALES A TRAVÉS DEL COMERCIO ELECTRÓNICO EN COLOMBIA.

Santiago Melo García

Tesis Presentada como requisito de grado para optar al título de:

Magíster en Derecho

Director:

Erick Rincón Cárdenas

Bogotá D.C., Colombia

2021

TABLA DE CONTENIDO

EL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA EN EL TRATAMIENTO DE DATOS PERSONALES A TRAVÉS DEL COMERCIO ELECTRÓNICO EN COLOMBIA.

1. RESUMEN

En la actualidad, es de vital importancia que las empresas adopten las medidas de seguridad necesarias para la protección de los datos personales de los clientes, proveedores, empleados, colaboradores o con quien se tenga algún tipo de vínculo, máxime aún si las empresas comercializan sus productos o servicios a través de las plataformas digitales mediante el comercio electrónico. Lo anterior, se logra con una Programa Integral de Gestión de Protección de Datos, con unas políticas de privacidad adecuadas y acordes con las necesidades de los empresarios y unas medidas de seguridad robustas que garanticen la privacidad de la información, en aras de salvaguardar los derechos fundamentales de las personas.

2. ABSTRACT:

Currently, it is vitally important that companies adopt the necessary security measures to protect the personal data of customers, suppliers, employees, collaborators or with whom there is some kind of link, especially if companies market their products or services through digital platforms through electronic commerce. The foregoing is achieved with adequate privacy policies and in accordance with the needs of employers

and robust security measures that guarantee the privacy of information, to safeguard the human rights.

3. PALABRAS CLAVES:

Comercio electrónico, habeas data, privacidad, empresa, redes sociales.

4. KEYWORDS

E-commerce, habeas data, privacy, company, social networks.

5. HOJA DE VIDA DEL AUTOR

Santiago Melo García Abogado egresado de la Universidad de Manizales, Especialista en Derecho Comercial de la Universidad del Rosario, con experiencia en medios de comunicación masiva y entidades sin ánimo de lucro. Actualmente, me encuentro desempeñando el cargo de Gerente y Representante Legal de la Asociación Nacional Acción Social Ejército Colombia.

6. DIRECCIÓN DE NOTIFICACIONES

- **Dirección**: Calle 159 #56-75 apartamento 1303 torre 10 Parque Central Colina
- **Correo Electrónico**: samega_93@hotmail.com

7. GLOSARIO (DEFINICIONES LEGALES)

- **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 sea objeto de Tratamiento.
- **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 si 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 en asocio con otros, decida sobre la base de datos y /o el tratamiento de los datos.
- **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Aviso de Privacidad:** Comunicación verbal o escrita generada por el Responsable dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de Información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

- **Dato Público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil, de las personas, a su profesión, u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Datos Sensibles:** 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 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.
- **Transferencia:** La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y en encuentra dentro o fuera del país.
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando

tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

- **Consumidor o usuario:** Toda persona natural o jurídica que, como destinatario final, adquiera, disfrute o utilice un determinado producto, cualquiera que sea su naturaleza para la satisfacción de una necesidad propia, privada, familiar o doméstica y empresarial cuando no esté ligada intrínsecamente a su actividad económica. Se entenderá incluido en el concepto de consumidor el de usuario.
- **Contrato de adhesión:** Aquél en el que las cláusulas son dispuestas por el productor o proveedor, de manera que el consumidor no puede modificarlas, ni puede hacer otra cosa que aceptarlas o rechazarlas.
- **Garantía:** Obligación temporal, solidaria a cargo del productor y el proveedor, de responder por el buen estado del producto y la conformidad del mismo con las condiciones de idoneidad, calidad y seguridad legalmente exigibles o las ofrecidas. La garantía legal no tendrá contraprestación adicional al precio del producto.
- **Información:** en materia de protección al consumidor, se entiende como todo contenido y forma de dar a conocer la naturaleza, el origen, el modo de fabricación, los componentes los usos, el volumen, peso o medida, los precios, la forma de empleo, las propiedades, la calidad, la idoneidad o la cantidad, y toda otra característica o referencia relevante respecto de los productos que se

ofrezcan o pongan en circulación, así como los riesgos que puedan derivarse de su consumo o utilización.

- **Producto:** Todo bien o servicio.
- **Productor:** quien de manera habitual, directa o indirectamente, diseñe, produzca, fabrique, ensamble o importe de productos. También se reputa productos, quien diseñe, produzca, fabrique, ensamble o importe productos sujetos a reglamento técnico o medida sanitaria o fitosanitaria.
- **Proveedor o expendedor:** quien de manera habitual, directa o indirectamente ofrezca, suministre, distribuya o comercialice productos con o sin ánimo de lucro.
- **Publicidad:** Toda forma y contenido de comunicación que tenga como finalidad influir en las decisiones de consumo.
- **Publicidad engañosa:** Aquella cuyo contenido no corresponda a la realidad o sea insuficiente, de manera que induzca o pueda inducir a error, engaño o confusión.
- **Seguridad:** Condición del producto conforme con la cual en situaciones y normales de utilización, teniendo en cuenta la duración, la información suministrada en los términos de la presente ley y si procede, la puesta en servicio, instalación y mantenimiento no presenta riesgos irrazonables para la salud o integridad de los consumidores. En caso de que el producto no cumpla

con requisitos de seguridad establecidos en reglamentos técnicos o medidas sanitarias, se presumirá inseguro.

- **Ventas a distancia:** son las realizadas sin que el consumidor tenga contacto directo con el producto que adquiere, que se dan por medios, tales como correo, teléfono, catálogo o vía comercio electrónico.
- **Mensaje de datos:** La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos ópticos o similares como pudieran ser entre otros, el Intercambio Electrónico de Datos (EDI), internet, el correo electrónico, el telegrama, el télex o telefax.
- **Comercio electrónico:** abarca las cuestiones suscitadas por toda 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 medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución, toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros, de construcción de obras, de consultoría, de ingeniería, de concesión de licencia; todo acuerdo de concesión o explotación de un servicio público, de empresa conjunta y otras formas de cooperación industrial o comercial, de transporte de mercancías o de pasajeros por vía área, marítima y férrea o por carretera.

- **Intercambio Electrónicos de Datos (EDI):** La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto.
- **Sistema de Información:** se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensaje de datos.
- **Empresa:** toda actividad económica organizada para la producción, transformación, circulación, administración o custodia de bienes, o para la prestación de servicios. Dicha actividad se realizará a través de uno o más establecimientos de comercio.

8. INTRODUCCIÓN

Justificación, problema y objetivos de la investigación

En los últimos años, ha sido de vital importancia y de gran trascendencia todo lo relacionado con la protección de los datos personales, entendidos como toda información que pueda estar asociada o vinculada a una persona, los cuales dependiendo su ámbito pueden tener la naturaleza de públicos, privados, semiprivados y sensibles, estos últimos acarrean una mayor protección. Para nadie es un secreto que, con la globalización, la apertura de los mercados, la aparición de nuevas tecnologías y plataformas digitales, el mercado y la economía han cambiado, por ejemplo, hace algunos años era casi imposible o tenía un elevado costo comunicarse con alguna persona que se encontrará fuera del país, en la actualidad estamos a un clic de distancia. Además, somos testigos de cómo la adquisición de bienes y servicios han evolucionado

a través de los tiempos, hemos comprado en tiendas físicas, por catálogos, televentas, redes sociales y en tiendas virtuales mediante plataformas digitales.

Esta globalización, según la teoría de Thomas Friedman (Friedman, 2005), fue generada por lo que él denominó 10 aplanadores: *"Los muros se derrumban y las ventanas se levantan"* (refiriéndose a la caída del muro de Berlín); "*Netscape sale a la bolsa"* (teniendo como referencia el 9 de agosto de 1995 día en el que el "World Wide Web" empezó a cotizar en la Bolsa y en el que según el autor "*el mundo no ha vuelto a ser el mismo"*); "*aplicaciones informáticas para el flujo del trabajo*"; "*el acceso libre a los códigos fuente*" (Open-sourcing); la "*Subcontratación*" (outsourcing); *"traslado de fábricas para abaratar costes*" (Offshoring); "*cadena de suministros*" (Supply-Chaining); "*Intromisión de los subcontratistas en las empresas contratantes*" (Insourcing); "*el acceso a la libre información*" (In-Forming) y; los "*esteroides*" (el autor utilizó este término para llamar así a las nuevas tecnologías que según el amplifican y aceleran la implementación de los demás aplanadores).

Esta situación, ha permitido la intercomunicación del hemisferio y ha beneficiado la economía de los países produciendo una mayor competitividad, que implica que los productores y proveedores de bienes y servicios adecuen sus procesos a las nuevas tecnologías.

Lastimosamente, el crecimiento económico y la competencia no es igual en todos los países, ya que existe una elevada desigualdad económica y sociocultural que impide a determinadas naciones en vía de desarrollo crecer en el mismo sentido de las grandes

potencias, aunado a la existencia de barreras arancelarias y no arancelarias, crisis humanitarias en fronteras, guerras, conflictos internos, entre otros aspectos. Al respecto, coincide la doctrina al resaltar que:

> *"a partir de la segunda mitad del siglo XX, la economía mundial y el comercio han girado en torno al fenómeno conocido como "Globalización", cuyos postulados y principios se basan en la búsqueda del desarrollo de los pueblos y el comercio libre. Esto ha sido posible gracias a la existencia de un idioma único-el inglés- y al avance de las telecomunicaciones, las cuales han permitido rápidamente realizar negocios debido a la masificación del intercambio electrónico de datos e internet"* (Castro, 2016).

Por su parte, las nuevas tecnologías han generado que los empresarios tengan que adecuar su cadena de producción y suministro para poder permanecer en el mercado. Con las TICS las empresas se vieron en la necesidad de ofrecer y comercializar sus productos a través del Comercio Electrónico, dejando en un segundo plano el comercio tradicional, lo que les permite tener un mayor alcance y que sus productos lleguen a una mayor cantidad de consumidores finales.

El comercio electrónico es definido por el estatuto del consumidor colombiano[1] en su artículo 49 como la *"realización de actos, negocios u operaciones mercantiles*

[1] Ley 1480 de 2011.

concertados a través del intercambio de mensajes de datos telemáticamente cursados entre proveedores y los consumidores para la comercialización de productos y servicios". Por otro lado, la ley 527 de 1997 en su artículo 2 lo define como las *"cuestiones suscitadas por toda 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 medio similar".*

Hoy en día, las empresas deben ir a la par de las nuevas tecnologías, ello les puede significar llegar a un mercado más amplio y aumentar el número de consumidores, todo esto con la implementación de los avances tecnológicos en toda la cadena de producción, es decir, desde la consecución de las materias primas, pasando por la etapa de fabricación y distribución, hasta en los mecanismos de publicidad y mercadeo para alcanzar la finalidad de que los productos lleguen a la mayor cantidad de personas posibles.

No obstante, lo anterior, las empresas colisionan con la realidad y ven como tristemente la regulación y normatividad que les garantice seguridad jurídica al momento de la implementación de las nuevas tecnologías, va un paso atrás, situación que desincentiva al empresario. Casos en Colombia como los de las aplicaciones de transporte urbano privado, permiten evidenciar esta circunstancia, ya que no hay una regulación específica que permita el normal desarrollo de la explotación de dichas plataformas digitales, lo que genera una inseguridad jurídica a los empresarios y usuarios que pueden ver afectado su capital y vulnerados sus derechos.

En cuanto a la aplicación de los avances tecnológicos en las empresas, el doctrinante Fernando Jiménez Valderrama, considera que:

> *"En el siglo XXI el valor de la tecnología y del conocimiento humano constituirán uno de los principales factores determinadores de la riqueza económica de las naciones, superando otros factores tradicionales como la capacidad de producción de materias primas o de productos manufacturados. Cada uno de estos renglones que, tradicionalmente integraban el concepto de riqueza, pierden paulatinamente valor frente al crecimiento desmesurado del valor de patrimonio tecnológico, que comienza a jerarquizar la comunidad de naciones en dos grupos, aquellas que poseen tecnología y aquellas que dependen tecnológicamente de las primeras"* (Valderrama, 2018).

Por lo tanto, veremos a lo largo de la investigación que las empresas no sólo deben preocuparse por la protección jurídica del conocimiento y la tecnología, tal como seria en todo lo relacionado con la marca, las patentes, los diseños industriales, los modelos de utilidad y el secreto profesional, entre otros, sino que deben también implementar políticas de buen gobierno corporativo y demás políticas que le permitan cumplir con su misión, visión y sus metas para una adecuada participación en el mercado.

Dentro de dichas políticas, se encuentra la de protección de datos personales, que tiene como finalidad garantizar el derecho fundamental del habeas data, establecido en el artículo 15 de la constitución política de Colombia, para que las personas puedan actualizar, rectificar, suprimir, conocer y eliminar su información personal, dentro de

un Estado Social y Democrático de Derecho, garante de los derechos fundamentales y libertades de todas las personas. Si bien, el derecho fundamental de habeas data fue incorporado en nuestro ordenamiento jurídico a partir de la constitución de 1991, solo hasta el año 2008 fue regulado parcialmente por el Congreso Nacional mediante la ley 1266 del 31 de diciembre de 2008 *"por la cual se dictan disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y proveniente de terceros países y se dictan otras disposiciones*" y posteriormente con la ley estatutaria 1581 del año 2012 "*por la cual se dictan disposiciones generales para la protección de datos personales"*, es decir, tuvo que pasar aproximadamente 21 años para que dicho derecho fuera protegido jurídicamente de una manera más efectiva.

Lo anterior, debido a que lastimosamente el crecimiento económico de nuestro país ha sido lento por diferentes motivos como el conflicto armado interno, el narcotráfico, la corrupción, factores económicos y culturales que impidieron la llegada de nuevas tecnologías a la velocidad en que llegaron a otros países, situación que ha sido superada poco a poco por la apertura económica que se dio a partir del año 1991 y por la reducción del conflicto armado interno que ha puesto a Colombia en la mira de grandes inversionistas.

Por otro lado, la información personal ha adquirido un valor invaluable, en especial en el comercio electrónico, ya que otorga la oportunidad de conocer de manera detallada los gustos, intereses e ideologías del consumidor final, para que las empresas

a través de las estrategias de publicidad y mercadeo se dirijan a consumidores y cumplan con su finalidad de ampliar su mercado. Sin embargo, este evento en la práctica creó grandes riesgos de seguridad y vulneración de la privacidad e intimidad de las personas, por lo que el Congreso Nacional, advirtió la necesidad de regular los aspectos de la protección de los datos personales con base en los postulados constitucionales.

De ahí, que lo que se busca con la presente investigación es realizar un análisis y dar recomendaciones acerca de los deberes y de las medidas de seguridad que deben adoptar las empresas que actúen como responsables y encargados del tratamiento de datos personales al momento de la promoción y comercialización de sus bienes y servicios a través del comercio electrónico, basados en el principio de responsabilidad demostrada que se encuentra inmerso en el régimen legal de protección de datos personales colombiano y con base en la ley del comercio electrónico, con el ánimo de reducir los riesgos que esta actividad genera para la intimidad, privacidad y seguridad de las personas por la divulgación de sus datos e información personal, al momento de hacer una transacción a través de las plataformas digitales.

Para lo cual y una vez planteado el problema, debemos preguntarnos ¿Cuáles son los deberes y las medidas de seguridad que deben adoptar las empresas como responsables y encargados del tratamiento de datos personales en cumplimiento del Principio de Responsabilidad Demostrada, al momento de la promoción y

comercialización de bienes y servicios a través del comercio electrónico, para evitar los riesgos que genera dicha actividad en la intimidad y privacidad en las personas?

Por lo tanto y para responder dicho interrogante, la primera tarea que tienen los empresarios es determinar que bases de datos manejan o van a manejar para el cumplimiento de su misión, las cuales generalmente contienen información de clientes, proveedores, personal, contratistas, ingreso de visitantes, información recolectada del "Newsletter" para la fidelización de los clientes, la recolectada en campañas de mercadeo y publicidad, y las demás que considere necesarias para el desarrollo adecuado de su negocio a través del comercio electrónico. Adicionalmente, deben determinar cuál es la información que se pretende recolectar, ya que dependiendo de ello deben adoptar diferentes medidas de seguridad para la protección de los datos personales, es decir, se debe determinar y clasificar la información en pública, privada, semiprivada y sensible. Recolección que en todo caso debe limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad que busca la empresa, tal y como lo establece el artículo 4 del Decreto 1377 de 2013.

Como se puede evidenciar, la protección de los datos personales trae consigo múltiples obligaciones que deben cumplir los responsables de la información, dentro de los cuales podemos encontrar a las empresas. Lastimosamente, es una ley que no ha tenido una suficiente pedagogía que permita su aplicación en todos los sectores de la sociedad, sin embargo, las personas debemos tener conciencia que el uso indebido de los datos personales e información que poseamos de terceras personas puede generar

la vulneración a la intimidad, dignidad humana, el derecho a la honra, al buen nombre e incluso inducir al suicidio.

De igual manera, muchos de los responsables del tratamiento de la información pensaron de manera errónea que sus obligaciones únicamente se reducían a redactar e implementar unas políticas de protección de datos personales y a realizar el registro de sus bases de datos en el RNBD, esto debido a como se mencionó anteriormente, a la falta de pedagógica al momento de la implementación de la normatividad aplicable. Es por esto que, se deben tener en cuenta cada uno de los deberes y obligaciones que tienen los responsables de la información, los cuales se encuentran establecidos en el artículo 17 de la ley 1581 de 2012.

Ahora bien, según la Superintendencia de Industria y Comercio, entidad de protección de Datos personales en Colombia, *"El Comercio Electrónico es el motor de la económica del siglo XXI y los datos personales son la moneda de la economía digital"* (Superintendencia de Industria y Comercio, 2019, pág. 1). Dicha frase, nos permite vislumbrar la importancia que tienen en el mercado actual el comercio electrónico y los datos personales, así como su vínculo estrecho e inseparable.

Por su parte, el Estatuto del Consumidor Colombiano (ley 1480 del 2011) establece un acápite especial en materia de protección al consumidor electrónico y una serie de obligaciones que se deben cumplir en el territorio nacional en el desarrollo de las actividades mercantiles de comercio electrónico, las cuales veremos más adelante.

Como se puede ver, las empresas que utilicen el comercio electrónico deben acatar no sólo las disposiciones que trae consigo el régimen de protección de datos personales, sino que además, deben cumplir con las obligaciones en materia de protección del consumidor electrónico, que da especial relevancia a la información de los consumidores en calidad de titulares y a los mecanismos de protección de la información implementados por las empresas como responsables del tratamiento de los datos personales.

Lo anterior, en aras de salvaguardar los derechos fundamentales de los consumidores electrónicos, generar la confianza entre ellos y los proveedores a través de las plataformas digitales, buscando reducir los riesgos a los que se encuentran los titulares de la información al momento de hacer la transacción mercantil electrónica, como por ejemplo la suplantación de la identidad, la filtración de información que pueda generar algún tipo de discriminación o poner en riesgo la vida de los titulares (datos sensibles), el hurto a través de las pasarelas de pago, la transferencia ilegal de los datos personales para provecho de terceros, que pueden poner en riesgo la seguridad, el buen nombre, la intimidad y el derecho de habeas data de las personas.

En efecto, es casi un manual el que deben cumplir los responsables del tratamiento de la información y es una ardua tarea que se debe desarrollar de manera conjunta con todas las áreas de una empresa. Es pues, una tarea mancomunada para garantizar todos los derechos de los titulares de la información y así evitar las sanciones

administrativas y/o pecuniarias que puede imponer la Superintendencia de Industria y Comercio, como entidad de protección de datos personales en nuestro país.

Por lo anterior, es recomendable que se revisen y se actualicen frecuentemente las políticas de privacidad, que sean diseñadas con base en el objeto social de la empresa y los principios rectores de la protección de los datos personales, que cumplan con todos los estándares y recomendaciones de la Superintendencia de Industria y Comercio.

De igual manera, dado el caso de que se presente una filtración de la información tratada o se presente una falla en las medidas de seguridad adoptadas, se informe dicha situación y las medidas que fueron adoptadas dentro del término establecido por la entidad de protección de datos personales.

Seguro que si se siguen todas estas recomendaciones, es probable que se reduzca el riesgo de un incumplimiento de la normatividad de datos personales que acarree sanciones pecuniarias y/o administrativas por parte de la Superintendencia de Industria y Comercio, entidad que entre agosto de 2018 y julio de 2019 impuso un total de 104 multas por un monto de $9.000 millones de pesos, debido al mal manejo de los datos personales (Díaz, 2019).

Cabe resaltar que dentro de las investigaciones más representativas sobre la materia que ha llevado a cabo la Superintendencia de Industria y Comercio se encuentra la de Facebook INC (Caso Facebook-Delegatura de Protección de Datos Personales, 2019),

que se inició en 8 países con ocasión a la publicación del 17 de marzo de 2018 realizada por el diario británico "The Guardian", en colaboración con los periódicos "The New York Times" y "The observer", mediante la cual se informó que Cambridge Analytica utilizó indebidamente los datos personales de más de 50 millones de usuarios de Facebook, vulneración que involucraba los nombres completos, edad, educación, intereses, historia laboral, cumpleaños, "Me Gusta"; localización física, fotos, estatus social, afiliaciones políticas y religiosas (datos sensibles) de los usuarios de esta red social, lo que le permitió a Cambridge Analytica Influenciar de manera confiable y manipular el comportamiento de los usuarios. Dicha vulneración, fue reconocida el 21 de marzo de 2018 por el señor Mark Zuckerberg, fundador y director ejecutivo de Facebook, quien anunció acciones tendientes a mejorar las medidas de seguridad de la plataforma. Posteriormente, Facebook informó a la Superintendencia de Industria y Comercio que la falla de seguridad sufrida en el caso de Cambridge Analytica, afectó la información personal de alrededor de 146.697 colombianos. Por este caso, la oficina del Comisionado de Información de Gran Bretaña (ICO) impuso una sanción monetaria de 500.000 libras esterlinas contra la red social.

Pero no sólo fue el caso de Cambridge Analytica el motivo de investigación a Facebook, también se llevó a cabo por el hurto de "tokens"[2] de acceso que permitía a

[2] Según el comunicado de Facebook realizado el 25 de septiembre de 2018, en donde informa la situación de vulneración, los "Tokens" de acceso, son el equivalente a llaves digitales que mantienen a

personas inescrupulosas tomar el control de las cuentas de 40 millones de sus usuarios, motivo por el cual la autoridad de protección de datos de Irlanda (The Data Protection Commission of Ireland-DPC), inició una investigación en contra de esta red social, la cual le fue notificada el 28 de septiembre de 2018.Adicionalmente, Facebook anunció el 14 de diciembre de 2018, una falla en el "Photo Api" que generó que terceros desarrolladores de aplicaciones, accedieran a las fotografías publicadas y no publicadas de 5,6 millones de usuarios sin la debida autorización, por lo que la DPC inició otra investigación el 17 de diciembre de 2018.

Por las vulneraciones a la protección de los datos personales descritas anteriormente, la Superintendencia de Industria y Comercio, argumentando que las medidas de seguridad de Facebook no son suficientes ni adecuadas para garantizar la seguridad de los datos personales de millones de personas, consideró necesario impartir a esta red social directrices preventivas con la finalidad de evitar que sucedan incidentes de seguridad que puedan afectar a sus usuarios en Colombia.

Otro de los casos de mayor renombre a nivel mundial fue el de UBER, presentado con ocasión al comunicado del señor Dara Khosrowshahi director ejecutivo (CEO) de dicha empresa, quien anunció públicamente en el año 2017 que un incidente de seguridad ocurrido en el año 2016, había afectado información personal almacenada en

---

las personas conectadas a Facebook y evitan que tengan que reingresar su clave cada vez que quieren usar la plataforma.

la nube de un proveedor externo (Amazon), relacionada con los nombres y los números de licencia de conducción de 600.000 conductores en Estados Unidos e información personal de 57 millones de usuarios alrededor del mundo, dentro de los cuales se estima que se encuentran 267.000 colombianos afectados. Por esta situación, la Oficina del Comisionado de Información de Gran Bretaña (ICO) le impuso a UBER una sanción pecuniaria de 385.000 libras esterlinas, asimismo, la Autoridad de Protección de Datos de los Países Bajos (Autoriteit Persoonsgegevens) le impuso una multa de 600.000 euros y, como si fuera poco, el 20 de diciembre de 2018 la Comisión Nacional de Informática y de las libertades de Francia (CNIL) impuso una multa de 400.000 euros a UBER FRANCE SAS., por el incumplimiento de la obligación de garantizar la seguridad de los datos personales frente al incidente de seguridad ya mencionado.

Por lo tanto, la Superintendencia de Industria y Comercio, a través de la Delegatura de Protección de Datos Personales, consideró que UBER falló en sus políticas y prácticas con la finalidad de garantizar de manera efectiva la protección de los datos personales almacenados en sus bases de datos, por el incidente de seguridad ocurrido entre octubre y noviembre de 2016, fallando en la implementación de medidas de seguridad suficientes y necesarias para impedir que terceras personas accedieran a la información personal almacenada, motivo por el cual impartió directrices con carácter preventivo dando la orden a UBER de implementar, mejorar o robustecer las medidas de seguridad para garantizar la protección de los datos personales, con el ánimo de evitar su acceso no autorizado o fraudulento, uso no autorizado o fraudulento, consulta

no autorizada o fraudulenta, la adulteración y/o su pérdida; entre otras directrices. (Caso UBER-Delegatura de Protección de Datos Personales, 2019)

En estos dos casos, los responsables de la información incumplieron con sus obligaciones, en especial, la contenida en el literal del artículo 17 de la ley 1581 de 2012, en el sentido de que tenían que *"conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento",* deber que también se encuentra en cabeza del encargado del tratamiento de los datos personales, que en el caso de UBER se trataba de AMAZON. Este deber es de carácter preventivo, lo que obliga tanto a los responsables como a los encargados a identificar los posibles riesgos para que puedan diseñar e implementar las medidas de seguridad conforme con las necesidades de su empresa. Asimismo, se pudo evidenciar que la protección de los datos personales es un tema de gran relevancia transfronteriza, por cuanto la mayor cantidad de datos personales son tratados en aplicaciones tecnológicas y redes sociales, que tienen su domicilio principal en diferentes partes del mundo.

Si bien en los casos expuestos anteriormente, la Superintendencia de Industria y Comercio no impuso sanciones pecuniarias sino que conminó a los investigados a cumplir con directrices preventivas en aras de mejorar la seguridad en el tratamiento de datos personales, en otros casos, si le impuso al Banco Falabella una multa por 496 millones de pesos y a Rappi una multa por 298 millones de pesos, dándoles la orden de adoptar medidas para respetar los derechos de las personas respecto del tratamiento de

los datos personales y en especial con lo relacionado a los derechos de supresión y atención debida de las solicitudes de los titulares (Superintendencia de Industria y Comercio, 2019)

En conclusión, el éxito del diseño y la implementación del plan y de las políticas de protección de datos personales, dependerá del compromiso efectivo de todos los miembros de una empresa, de que el mismo sea diseñado como si fuera un traje hecho a la medida de la compañía, que evalúe y evite los riesgos y que blinde jurídicamente a la organización dentro del marco del cumplimiento de su objeto social y, en especial cuando se implemente el sistema de comercio electrónico. Para tal fin, es de vital importancia que la alta dirigencia de una empresa sea proactiva para que con las iniciativas propias y con la destinación respectiva de los recursos, adopten medidas estratégicas de alto impacto para garantizar efectivamente el derecho al habeas data tanto de sus empleados y/o sus contratistas, como la de sus clientes y proveedores.

9. METODOLOGÍA DE LA INVESTIGACIÓN

La metodología escogida para el desarrollo del proyecto de investigación es la descriptiva, con la que se busca analizar y describir los conceptos propios del régimen de protección de datos personales y del comercio electrónico, para establecer si en Colombia las empresas que actúan como responsables y encargados del tratamiento de los datos personales, cumplen con sus deberes y establecen las medidas necesarias para la protección de los datos personales (principio de responsabilidad demostrada), evitando vulnerar los derechos fundamentales de las personas como la intimidad y el

buen nombre, teniendo en cuenta un análisis descriptivo cualitativo de las sanciones impuestas por la Superintendencia de industria y Comercio a las empresas que incumplen con sus deberes como responsables del tratamiento de datos personales en el desarrollo del comercio electrónico, para llegar a una serie de conclusiones y emitir unas recomendaciones tendientes al cumplimiento del principio de responsabilidad demostrada que trae consigo el Régimen de Protección de Datos Personales Colombiano.

10. GENERALIDADES DE LA PROTECCIÓN DE DATOS PERSONALES

Origen

Para empezar, es indispensable abarcar las generalidades que trae consigo el régimen de protección de datos personales en Colombia y la vital importancia de la información en nuestros días, partiendo de su origen, evolución y haciendo un estudio detallado del contenido de la normatividad, con el ánimo de ilustrar la importancia sobre la materia en el ordenamiento de nuestro país al momento de proteger los derechos fundamentales de las personas, para iniciar con el recorrido del camino que nos lleve hacia los principios que rigen la protección de datos personales, en especial el principio de responsabilidad demostrada y así establecer el vínculo que este tema tiene con el Comercio Electrónico.

En primer lugar, cabe resaltar que la información de las personas tiene un valor trascendental para el desarrollo de las actividades comerciales de las empresas, ya que

permite su identificación al momento de las transacciones, dar a conocer cuáles son sus gustos e intereses y permite su diferenciación de los demás en una sociedad, lo cual es importante al momento de desarrollar campañas de mercadeo y tomar decisiones administrativas basadas en estadísticas de consumo. Así, lo han resaltado los doctrinantes Bruno J. Gaiero e Ignacio M. Soba, al considerar que: "*la información tiene gran relevancia en la determinación y planificación de la conducta diaria de los individuos. Es bien sabido que la información habilita a determinar la conducta propia y ajena y que la concentración de información se transforma, así en un reducto incuestionable de poder"* (Gaiero & Soba , 2010).

De ahí, radica la importancia de que las empresas establezcan herramientas y medidas adecuadas que garanticen la protección de los datos personales, con el ánimo de evitar perjuicios a los titulares y en esa medida cumplir con su objeto social y llegar a un mayor número de consumidores con estrategias que le permitan dar a conocer sus productos o servicios.

De lo anterior se puede desprender que la información es importante para el desarrollo de todos los sectores de la sociedad, es lo que permite crear vínculos entre las personas, entre las personas y las empresas, así como las personas con el estado para el cumplimiento de sus fines esenciales. La información de las personas, constituye una fuente de recursos para las empresas, redes sociales y para el estado, para adoptar sus estrategias y para la adecuada toma de decisiones, motivo por el cual el derecho fundamental al habeas data limita, protege y se considera como un medio

de defensa contra el tratamiento inadecuado de los datos personales por parte de las personas, empresas y entidades estatales que actúen como responsables del tratamiento de la información.

En cuanto su origen, los doctrinantes Bruno J. Gaiero e Ignacio M. Soba (Gaiero & Soba , 2010), así como Vivian Newman Pont (Newman, 2015), coinciden en que se da desde la obra clásica The rigth to privacy de Warren y Brandeis, quienes estudiaron el derecho a ser dejado en paz (the right to be let alone), derecho que se encontraba intrínsecamente vinculado a la intimidad de las personas, por lo que se puede deducir que el habeas data tenía una concepción única garante del derecho de la intimidad. Los doctrinantes anteriormente mencionados, al hacer un recuento histórico desde la época de la inquisición, las guerras mundiales, las revoluciones, hasta llegar a la globalización y a la implementación de nuevas herramientas tecnológicas, llegaron a la conclusión de que la información ha sido de gran relevancia y que las ventajas del manejo de esta son innumerables.

Por lo anterior, tanto las personas, como las empresas y el estado, con el devenir del tiempo y los cambios culturales, así como con la implementación de nuevas tecnologías y herramientas, se han visto en la necesidad de adoptar medidas para la protección de la información y de irlas adecuando a los diferentes cambios sociales. Por su parte, los estados y las organizaciones internacionales, han incorporado en sus constituciones, leyes, resoluciones y directivas tendientes a garantizar el adecuado tratamiento de los datos personales de las personas, cuya génesis y como lo pasaré a explicar más

adelante, fue la Declaración Universal de los Derechos Humanos proclamada el 10 de diciembre de 1948 con el reconocimiento del derecho a la intimidad, el cual fue reproducido en el Pacto Internacional de Derechos Civiles y Políticos y en la Convención Americana de Derechos Humanos de 1969.

Asimismo, en Europa se expidió la Resolución 65/509/CE del Consejo Europeo en la que se estudió la protección de la privacidad en las nuevas tecnologías. También, con la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, los estados miembros se comprometieron a garantizar la "*protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular del derecho a la intimidad, en lo que respecta al tratamiento de Datos Personales"*, además, se comprometieron a no "*restringir ni prohibir la libre circulación de datos personales entre los Estados Miembros".*

Marco Constitucional y normativo en Colombia

En Colombia, el derecho fundamental del habeas data, se encuentra establecido en el artículo 15 de la Constitución Política de 1991, que fue consagrado con la finalidad de que las personas puedan actualizar, rectificar, suprimir, conocer y eliminar su información personal, dentro de ese Estado Social de Derecho, garante de los derechos fundamentales y libertades de todas las personas para el cumplimiento de sus fines esenciales. Al respecto el precitado artículo establece lo siguiente:

> *(…) "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual*

modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley" (...).

Como se puede vislumbrar y al momento de hacer una discriminación detallada, en el precitado artículo se desarrollan los siguientes postulados:

1. El derecho a la intimidad Personal y Familiar.

2. El derecho al buen nombre.

3. El Derecho al Habeas Data en estricto sentido.

4. El carácter de inviolabilidad como regla general de la correspondencia y demás formas de comunicación privada y las excepciones a esta regla.

5. La exigibilidad de la presentación de libros de contabilidad y documentos privados dentro de la facultad de inspección, vigilancia y control, que en

principio está en cabeza del presidente de la República, quien la delegó a las Superintendencias y/o alcaldías y gobernaciones (en el caso de las Entidades Sin Ánimo de Lucro).

Adicionalmente, se establece que para el adecuado tratamiento de los datos personales, se respetarán la libertad y demás garantías consagradas en la Constitución Política. Sin embargo, se han visto casos en los que la intimidad puede colisionar con otros derechos como por ejemplo con el derecho de libertad, prensa e información, establecido en el artículo 20 de la Constitución Política, situación que se puede resolver con base en lo que Robert Alexy denomina la Ponderación, que es la manera en la cual se armonizan los principios en determinados casos concretos.

En un principio y tal como se explica en la Sentencia C-748 de 2011 (Cconst, C-748/2011, J. Pretelt) proferida por la Corte Constitucional y en la que se estudió la Constitucionalidad de la ley estatutaria 1581 de 2021 (Régimen General de Protección de Datos Personales), la jurisprudencia consideró al Habeas Data como una garantía integradora del derecho a la intimidad, posteriormente, como una manifestación del libre desarrollo de la personalidad y en una tercera línea interpretativa lo consideró como un derecho autónomo, postura que ha prevalecido desde 1995 hasta la fecha.

En relación con esta última postura, la Corte Constitucional en la precitada jurisprudencia, cita la sentencia C-1011 de 2008 que reconoció nuevamente la autonomía del derecho al habeas data, conceptualizándolo de la siguiente manera:

> *"El hábeas data confiere, (…), un grupo de facultades al individuo para que, en ejercicio de la cláusula general de libertad, pueda controlar la información de sí mismo ha sido recopilada por una central de información. En ese sentido, este derecho fundamental está dirigido a preservar los intereses del titular de la información ante el potencial abuso del poder informático" (Cconst, C-1011 de 2008, J. Córdoba).*

En síntesis, a pesar de que exista relación entre el derecho a la intimidad, el buen nombre, el libre desarrollo de la personalidad y el Habeas Data, no significa que este último sea un derecho diferente, ya que comprende unas garantías diferenciales y puede ser reclamado directamente por medio de la acción de tutela, tal como lo ha resaltado la jurisprudencia.

Como se mencionó anteriormente, el habeas data que tiene como finalidad la protección de los datos personales, tiene su génesis en el derecho de la intimidad humana, al que se encuentra estrechamente vinculado y el cual fue reconocido internacionalmente por primera vez en la Declaración Universal de los Derechos Humanos, proclamada el 10 de diciembre de 1948, en cuyo artículo 12 se estableció que "*nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su*

domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley en contra tales injerencias o ataques". Este derecho, también fue consagrado posteriormente en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966.

El concepto de Habeas Data como tal, se empezó a estudiar de manera más detallada en el continente europeo, con base en la Resolución 509 de 1968 del Consejo de Europa, que se expidió debido a los riesgos existentes en la protección de la privacidad de las personas derivada de la implementación y el uso de nuevas tecnologías. Posteriormente, con el Convenio 108 del Consejo de Europa de 1981 se fijó el modelo de protección del tratamiento automatizado de los datos personales, años más tarde, el Parlamento Europeo y el Consejo de Europa, mediante la Directiva 95/46/CE DE 1996, precisaron varias definiciones y directrices relacionadas con el tratamiento y circulación de Datos personales, situación que también fue consagrada en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

En Colombia, si bien en el artículo 15 de la Constitución Nacional no se menciona la expresión "Habeas Data", es importante resaltar que esta se encuentra en el artículo 42 del Decreto 2591 de 1991 *"por el cual se reglamenta la acción de tutela consagrada en el artículo 86 de la Constitución Política".*

Tiempo después, mediante la ley 1266 del 31 de diciembre de 2008 se reguló este derecho específicamente para la protección de la información crediticia, financiera y comercial de las personas. Sin embargo, este ámbito tan limitado que dio lugar a una regulación específica obligó al Congreso a regular el Derecho al Habeas Data mediante la ley 1581 de 2012 "*por la cual se dictan disposiciones generales para la protección de datos personales"*.

Cabe resaltar que se trata de una ley estatutaria, ya que regula un derecho fundamental y es aplicable para el tratamiento de los datos personales que se encuentren en cualquier base de datos administrada por cualquier entidad de naturaleza pública o privada en el territorio colombiano. Además, se establecieron los derechos de los titulares de la información, así como los deberes tanto de los responsables como de los encargados de esta.

No obstante lo anterior, no es un derecho absoluto ya que tiene unos límites materializados en las excepciones de aplicación del régimen de protección de datos personales, las cuales se encuentran consagradas en el artículo 2 de la precitada ley, como lo son las bases de datos mantenidas en un ámbito personal o doméstico; las que tengan por finalidad la seguridad y defensa nacional; las que contengan información de inteligencia y contrainteligencia; las bases de datos con información periodística; las que se encuentran bajo el régimen de protección de datos personales de información crediticia de la ley 1266 de 2008; así como las que se encuentran relacionada con los censos de población y vivienda en todo el territorio nacional. Sin embargo y en

concordancia con lo establecido en la ley, a estas bases de datos exceptuadas también le son aplicables los siguientes principios sobre la protección de datos personales: a) principio de veracidad o calidad de los registros de datos; b) principio de finalidad; c) principio de circulación restringida; d) principio de temporalidad de la información; e) principio de interpretación integral de derechos constitucionales; f) principio de seguridad; y g) principio de confidencialidad. Estos principios serán objeto de estudio en el siguiente acápite dada su importancia y relación con el tema de investigación.

El propósito de esta ley general de habeas data, es garantizar el adecuado tratamiento de los datos personales que son recolectados en Colombia y, en especial, garantizar el cumplimiento de los derechos de los titulares de la información de conocer, actualizar y rectificar sus datos personales frente a los responsables de llevarlo a cabo; solicitar al Responsable la prueba de la autorización otorgada para el tratamiento de los datos personales cuando así se requiera; informar respecto del uso que se le ha dado la información por parte de los responsables o encargados; así como a presentar quejas ante la Superintendencia de Industria y Comercio por infracciones a la ley de protección de datos; a revocar la autorización o solicitar la supresión de los datos cuando no se respeten las garantías constitucionales y legales y; a acceder en forma gratuita a los que hayan sido objeto de tratamiento.

La ley general de protección de datos personales, fue reglamentada parcialmente por el decreto N°1377 de 2013, en aspectos como la autorización del titular de la información para el adecuado tratamiento, las políticas de privacidad, el ejercicio de

los derechos de los titulares, las transferencias de datos personales y el principio de responsabilidad demostrada.

Definición de Dato Personal

En relación con la definición de dato personal, el artículo 3 de la ley 1266 de 2008 señala que se trata de *"cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica*", asimismo, el artículo 3 la ley 1581 de 2012 lo establece como *"cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"*. Los datos personales permiten identificar a las personas, conocer sus gustos, sus intereses, su círculo social, sus proyectos de vida frente a la sociedad, motivo por el cual, un inadecuado tratamiento de la información puede causar graves perjuicios económicos y morales a los titulares y a sus familias. Ahora bien frente a su composición y caracterización, Vivian Newman Pont (Newman, 2015, pág. 25) al analizar las definiciones legales de dato personal, cita las siguientes características que este tiene, con base en lo establecido en la sentencia T-729 de 2002 proferida por la Corte Constitucional: *a) "Se refiere a aspectos propios y exclusivos de una persona natural, b) ayuda a identificar a una persona en mayor o menor medida; c) su propiedad reside permanentemente en cabeza del titular del mismo, d) su tratamiento está sometido a principios en cuanto s su captación, administración y divulgación".*

Otra definición más completa y acorde con los avances tecnológicos, es la que da el Comité Jurídico Interamericano (CJI) de la Organización de los Estados Americanos (OEA) en el reciente informe sobre Principios Actualizados sobre la privacidad y la protección de datos personales, al considerar que este término abarca:

> (…) "*la información que identifica o puede usarse de manera razonable para identificar a una persona física de forma directa o indirecta, especialmente por referencia a un número de identificación, datos de localización, un identificador en línea o a uno o más factores referidos específicamente a su identidad física, fisiológica, genética, mental, económica, cultural o social. Incluye información expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica, electrónica, visual o de cualquier otro tipo. La frase no abarca la información que no identifica a una persona en particular (o no puede usarse de manera razonable para identificarla)"* (…) (Comité Jurídico Interamericano CJI de la Organización de los Estados Americanos, 2021).

Clases de Datos Personales

En cuanto a las clases de datos personales que pueden ser objeto de tratamiento, se puede hablar de información pública, entendida como aquella que se encuentra asociada al estado civil de las personas y a las que se encuentren en registros públicos, que por su naturaleza no se requiere autorización por parte del titular de la información.

Los Datos sensibles, según lo establecido en el artículo 5 de la ley 1581 de 2012 y en el artículo 3 del Decreto 1377 de 2013, son entendidos:

"*como 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"*

La ley establece que por regla general, que el tratamiento de los datos sensibles se encuentra prohibido salvo en aquellos casos en que su titular haya dado su autorización explícita; sea necesario para salvaguardar la vida del titular que se encuentre física o jurídicamente incapacitado; el tratamiento sea efectuado por ONGS o entidades sin ánimo de lucro cuya finalidad sea política, filosófica o sindical siempre que se refieran a sus miembros; sean necesarios para el reconocimiento o ejercicio de un derecho en un proceso judicial o; tenga una finalidad historia, estadística o científica.

Por lo tanto, los datos sensibles por su naturaleza merecen de una especial protección por parte de los responsables y/o encargados del tratamiento de los datos personales, que valga aclarar, no son las personas que se delegan dentro de la empresa para el tratamiento, sino que es la empresa como tal y/o sus aliados comerciales a los que les haya transferidos los datos personales administrados por su compañía.

Los denominados datos semiprivados, con base en las definiciones dadas en el artículo 3 del decreto 1377 de 2013, son aquellos que no tienen la naturaleza íntima, reservada o pública y su conocimiento puede interesar a su titular o a cierto grupo de personas. Los Datos privados, son aquellos que, por su naturaleza íntima o reservada, solo son relevantes para el titular de la información.

Autorización para el tratamiento de los datos personales

Una vez analizadas las definiciones de los diferentes tipos de datos personales que se pueden recolectar, se debe aclarar que únicamente los datos públicos no requieren para su tratamiento la autorización por parte del titular de la información. De aquí, tiene su fundamento otra de las obligaciones en cabeza de los responsables y de los encargados, que es la de obtener la autorización previa, expresa e informada que los habilite para el uso y tratamiento de los datos personales recolectados, teniendo en cuenta que, según la normatividad en la materia, no se pueden utilizar medios engañosos para recolectarlos y tratarlos.

Dicha autorización, deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior, puesto que uno de los derechos de los titulares de la información, es solicitarle al responsable la prueba de la misma, además, la Superintendencia de Industria y Comercio puede solicitarla como prueba dentro de los procesos administrativos sancionatorios en ejercicio de sus facultades legales, constituyéndose

en una prueba fundamental que en muchas ocasiones puede absolver al Responsable o Encargado que se encuentran siendo investigados.

Para tal fin, las empresas en su calidad de responsables del tratamiento de la información cuentan con la libertad de adoptar los mecanismos necesarios para la obtención de la autorización del tratamiento de los datos personales, dependiendo de su infraestructura y su capacidad económica, pero siempre deben tener en cuenta que la misma debe ser archivada con medidas de seguridad pertinentes que permitan su consulta posterior, ya que como lo dijimos anteriormente, eventualmente puede ser requerida por el titular, sus causahabientes o por parte de la Superintendencia de Industria y Comercio que es la entidad encargada en Colombia de la vigilancia y control de la protección de los datos personales.

Sin embargo, la ley de Protección de Datos Personales trae consigo los casos en los que no es necesaria la autorización del tratamiento, por tratarse de:

> *"a) información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; b) datos de naturaleza pública; c) casos de urgencia médica o sanitaria; d) tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; e) datos relacionados con el registro civil de las personas".*

La autorización es quizás uno de los deberes más importantes que tienen los responsables y encargados del tratamiento de la información, puesto es la prueba que los habilita y los legitima para usar los datos personales recolectados para los fines específicos. Adicionalmente, da la potestad a los titulares de la información para que de manera previa e informada y sin ningún tipo de coacciones tomen la decisión de entregar o no sus datos personales a las entidades públicas o privadas que los requieran. Las empresas deben adoptar los mecanismos técnicos y administrativos conforme con su objeto social y su estructura, para solicitar de manera adecuada y por cualquier medio la autorización del tratamiento de los datos personales por parte de los titulares, así como para almacenarla durante el tiempo requerido para el cumplimiento de las finalidades del tratamiento. Esta autorización puede darse por diferentes medios como formularios físicos, llamadas telefónicas, mensajes de texto, biometría, aceptación de términos y condiciones en la página web.

En todo caso y con base en la normativa en la materia, es deber de los responsables informar a los titulares de manera clara el tratamiento que le darán a los datos personales, los derechos que le asisten, así como los datos de ubicación y contacto de los responsables. Además, la autorización debe ser una autorización expresa, es decir, no debe ser tácita como por ejemplo sería dar a entender que si en determinado tiempo no se da respuesta a la solicitud de autorización o diligenciamiento de un formulario, se da por hecho que el titular aceptó el tratamiento de los datos personales. Por lo anterior y con base en lo establecido en el artículo 7 del decreto 1377 de 2013, se

entenderá que la autorización es válida y cumple con la totalidad de los requisitos cuando se manifieste *"(i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca".*

Deberes de los Responsables y Encargados del Tratamiento de los Datos Personales

Ahora bien, de conformidad con lo establecido en el artículo 17 de la ley 1581 de 2012, son deberes de los responsables del tratamiento de los datos personales:

(...) a) "Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) solicitar y conservar, en las condiciones previstas en la presente le, copia de la respectiva autorización otorgada por el Titular.

c) informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

d) conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar 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,

g) rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.

h) suministrar al Encargado del tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.

K) Adoptar 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.

l) Informar 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.

m) Informar a solicitud del titular sobre el uso dado a sus datos.

n) Informar 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.

o) cumplir las instrucciones y requerimiento que imparta la Superintendencia de Industria y Comercio". (…)

De igual manera, la precitada normatividad en su artículo 18 trae consigo los deberes de los encargados del tratamiento de los datos personales, entendidos como aquellos que realizan el tratamiento por cuenta de los responsables. Dichos deberes son los siguientes:

a) Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.

d) actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.

e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley.

f) adoptar 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 por parte de los titulares.

g) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley.

h) insertar en la base de datos la leyenda "Información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.

i) abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

j) permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

k) informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de los titulares.

l) cumplir las instrucción y requerimientos que imparta la Superintendencia de Industria y Comercio".

Como puede observarse, son muchos los deberes y responsabilidades que tienen tanto los responsables del tratamiento de los datos personales como los encargados de este. Esta distinción es importante, dado que en el giro ordinario de los negocios

muchas empresas realizan distintos actos jurídicos en los que se ven involucrados datos personales que se encuentran recolectados en sus bases de datos. Esta situación es muy común e incluso existen varios ejemplos de ello, como lo seria cuando las empresas contratan con otras para realizar el análisis de hojas de vida para ocupar una vacante existente, o cuando se contrata con una empresa de mercadeo o de publicidad para realizar diferentes campañas publicitarias y para ello requieren la información de la base de datos de los clientes, o cuando se contrata una pasarela de pagos para la implementación de la plataforma de comercio electrónico que permita las transacciones y se requiere tener acceso a información crediticia de los clientes.

En estos casos, también compete a los responsables tener una debida diligencia al momento de seleccionar a los contratistas, verificar que cuenten con políticas de privacidad y con medidas de seguridad robustas que permitan realizar un adecuado tratamiento de datos personales. De igual manera, se requiere que los responsables tengan autorización expresa por parte de los titulares para la transferencia de los datos a los encargados y que tal disposición se encuentre de manera taxativa en las finalidades informadas previamente. Además, que en los contratos celebrados entre los responsables y encargados, se encuentren establecidas cláusulas de protección de datos personales y acuerdos de confidencialidad que blinden jurídicamente el vínculo contractual que los une. En este punto y tal como lo señala la ley de datos personales, pueden concurrir las calidades de responsable y encargado en una misma persona, caso en el cual, le será exigible el cumplimiento de los deberes previstos para cada uno. Al

respecto y en relación con la concurrencia de calidades y responsabilidad de los responsables y encargados del tratamiento de los datos personales, Pedro Pablo Camargo (Camargo, El Habeas Data , 2013), resaltó que:

> *"La corte, en su sentencia C-748/2011 reitera, tal como lo dejó consignado en su sentencia C-1011 /08 , que tanto el responsable como el encargado del tratamiento tienen una responsabilidad concurrente frente a la veracidad, integridad, fidelidad e incorporación del dato, si se tiene en cuenta que la recolección y procesamiento de datos no es una actividad neutra que impida al encargado del tratamiento responder, incluso por la veracidad de la información sujeta a proceso pues a este le corresponde cerciorarse de que se cumplan los requisitos para que un dato personal pueda ser objeto de tratamiento"*
>
> *"En consecuencia, la sala advierte que si no se puede identificar de forma clara la posición de uno y otro, tendrán que responder de forma solidaria y no podrán excusar sus deberes de actualización, rectificación y exclusión o supresión del* dato".

Políticas de Protección de Datos Personales

Dentro de las precitadas obligaciones y deberes que tienen los responsables y encargados del tratamiento de la información, está la de la implementación de políticas de protección de datos personales o las llamadas políticas de privacidad, las cuales deben cumplir con el contenido establecido en la ley 1581 de 2012 y en el artículo 13

del decreto 1377 de 2013, ya que requieren de ciertos formalismos en aras de garantizar los derechos de los titulares de la información. En otras palabras, la política de protección de datos personales debe contener como mínimo lo siguiente:

- Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del responsable.
- Tratamiento al cual serán sometidos los datos y finalidad de este, salvo que ya se haya informado mediante aviso de privacidad.
- Derechos de los titulares de la información.
- Persona o área responsable de la atención de las peticiones, consultas y reclamos del titular de la información.
- Procedimiento para el ejercicio de los derechos que tienen los titulares.
- Fecha de entrada en vigor de la política de tratamiento de la información y periodo de vigencia de la base de datos.

Cualquier cambio sustancial que realice el responsable o el encargado a las políticas de tratamiento de datos personales, debe ser comunicado de manera oportuna y previa a su implementación a los titulares de la información.

En todo caso, las políticas del tratamiento de los datos personales conforme con lo establecido en el artículo 13 del decreto 1377 de 2013, deben constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los titulares. Asimismo, es importante tener en cuenta que en el caso en que no sea posible poner a disposición del titular las políticas de tratamiento de la información, los

responsables deberán informar mediante aviso de privacidad la existencia de tales políticas y el mecanismo para acceder a ellas. Aquí, también vemos la libertad con que cuentan las empresas para dar a conocer las políticas y el aviso de privacidad, ya que lo pueden hacer a través de documentos, formatos electrónicos, de manera verbal o cualquier tecnología, lo importante es que el titular se encuentre informado de la existencia de estas y los derechos que le conceden.

Registro Nacional de Base de Datos

Otro aspecto importante que trae la ley de protección de datos personales es la creación del Registro Nacional de Base de Datos (en adelante el RNBD), administrado por la Superintendencia de Industria y Comercio, el cual fue creado con el propósito de garantizar el derecho a los titulares, para que los mismos conozcan quienes son los responsables del tratamiento de su información.

Cabe resaltar que es una obligación de algunos responsables del tratamiento de la información, inscribir las bases de datos con que cuentan en el RNBD, para lo cual la Superintendencia de Industria y Comercio estableció unos términos, que a la hora de la implementación tuvo que modificar debido a las dificultades con que contaban los responsables de la información para hacer el correspondiente registro, ya que no era un trámite sencillo y requería de un trabajo interno tedioso tendiente a organizar e identificar las bases de datos con que se contaban y a obtener la autorización del tratamiento de los datos personales de los titulares que en ella se encontraban. Poco a

poco, la Superintendencia de Industria y Comercio entendió que no era un proceso para desarrollar de la noche a la mañana, de igual manera hizo un estudio detallado para reducir el número de los responsables que debían realizar dicho registro, considerando el patrimonio y el tamaño de las empresas.

Autoridad de Protección de Datos en Colombia

En cuanto a la inspección, vigilancia y control, la ley 1581 de 2012, en su artículo 19 establece que la autoridad de protección de datos en Colombia es la Superintendencia de Industria y Comercio a través de la Delegatura de Protección de Datos Personales, quien en el ejercicio de sus funciones garantiza que se respeten los principios, derechos y garantías de mencionada ley. Sin embargo, muchas han sido las críticas frente a la delegación de estas facultades en cabeza de la Superintendencia de Industria y comercio, por ser una entidad perteneciente a la rama ejecutiva del poder Público, situación que pone en riesgo la separación de poderes y va en contravía de la independencia y del principio de imparcialidad, máxime aún, que las entidades estatales son las que realizan el tratamiento de la mayor parte de los datos personales en el país, y a estas le son aplicables las disposiciones legales en esta materia. Esta crítica, entre otras, fue manifestada en el salvamento de voto de la sentencia C-748 del 2011 por los magistrados de la Corte Constitucional María Victoria Calle, Jorge Iván Palacio y Luis Ernesto Vargas y, además, por varios doctrinantes como por ejemplo

Pedro Pablo Camargo en su libro denominado “El Habeas Data” (Camargo, El Habeas Data , 2013, pág. 107)

Esta situación que afecta la independencia también fue advertida por la Organización para la Cooperación y el Desarrollo Económico (OCDE) al momento de estudiar la adhesión de Colombia que inició en el año 2021, tal y como lo narró Mauricio Cárdenas en su libro “Como Avanza Colombia” de la siguiente manera: *“Según la OCDE, que el presidente de la República pueda remover a los superintendentes por presiones políticas cuando toman medidas incómodas para los vigilados es algo que le resta independencia a su labor*” (Cárdenas, 2021).

Adicionalmente y según lo señalado en el artículo 21 de la ley 1581 de 2012, la Superintendencia de Industria y Comercio entre otras actividades, vela por el cumplimiento de la legislación aplicable a la protección de los datos personales; adelanta las investigaciones y toma las medidas necesarias para hacer efectivo el derecho de habeas data; dispone el bloqueo temporal de los datos cuando sea necesario para proteger los derechos fundamentales de los titulares de la información; promueve y divulga los derechos de las personas en relación con el tratamiento de los datos personales a través de campañas pedagógicas; imparte instrucciones sobre las medidas y procedimientos a los Responsables y encargados del Tratamiento; solicita a los Responsables y a los Encargados información para el cumplimiento de sus funciones; profiere las declaraciones sobre la transferencia internacional de datos; administra el Registro Nacional Público de Bases de Datos y emite las órdenes y los actos necesarios

para su administración y su funcionamiento, sugiere los ajustes o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, requiere la colaboración de las entidades intencionales cuando se afecten los derechos de los titulares fuera del territorio colombiano, y debe cumplir con las demás funciones que le sean asignadas por ley.

Sanciones que puede imponer la Autoridad de Protección de Datos en Colombia

En relación con las sanciones que pude imponer la Superintendencia de Industria y Comercio, previo cumplimiento de las etapas procesales y garantía del debido proceso, el artículo 23 de la ley de protección de datos personales establece las siguientes:

(…) "a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó; b) suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar; c) cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio; cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles". (…)

Es por esto que en el caso de que una empresa como responsable de la información no cumpla con sus deberes legales y se materialice un incidente de seguridad que ponga en riesgo la información personal de los titulares, la empresa se verá expuesta a una sanción pecuniaria y administrativa por parte de la Superintendencia de Industria y Comercio. Una filtración de la información de los titulares puede acarrear elevados costos a las empresas responsables, presupuesto que puede ser destinado al fortalecimiento de la infraestructura y adoptar previamente medidas de seguridad, con el ánimo de evitar este tipo sanciones. Sin embargo, no solo son las multas que impone la entidad reguladora la que genera grandes costos, sino que también lo son la pérdida de la confianza de los clientes, la reducción de la valorización de las acciones, honorarios de representación legal, notificaciones a los titulares y a la superintendencia de industria y comercio, entre otros factores que pueden hacer más gravosa la situación económica de la empresa sancionada. En consecuencia, siempre se recomienda que las empresas adopten las medidas de seguridad preventivas que generen confianza en los consumidores.

Al respecto, Paloma Llaneza en su libro denominado “Datanomics” (Llaneza, 2019, pág. 270), expone las siguientes cuatro actividades o centros de costo que son identificados por el Instituto Ponemon, relacionado con incidentes que ponen en riesgo la información personal de los titulares:

(...) 1. Detección y Escalado: "aquí se incluyen las actividades que permiten a una empresa detectar y reportar la violación de seguridad al personal apropiado dentro de un determinado período de tiempo, como, por ejemplo, las actividades forenses y de investigación; los servicios de evaluación y auditoría; la gestión de equipos de crisis, y las comunicaciones a la dirección ejecutiva y el consejo de administración.

2. Costes de Notificación a las personas afectadas por la brecha de datos, como, por ejemplo, remisión de correos electrónicos, cartas, llamadas telefónicas o, en general, cualquier notificación sobre la información personal que se ha perdido o robado; y la comunicación al regulador.

3. Respuesta posterior a la brecha de datos y, en concreto, la ayuda de los afectados por la fuga de datos para resolver los problemas que les haya causado como, por ejemplo, servicios de seguimiento para saber si se ha usado la información en perjuicio del afectado, servicios de protección de identidad o de apertura de nuevas cuentas o emisión de tarjetas de crédito, los gastos legales en los que hayan incurrido, así como posibles descuentos en los productos o servicios de la empresa.

4. Pérdida de ingresos por pérdida de confianza de los clientes, pérdidas por la paralización de los sistemas informáticos, así como los costes de pérdida de clientes y los gastos necesarios para recuperarlo o conseguir nuevos clientes". También se

incluye el cálculo de la pérdida de negocio por la afectación de la reputación de la compañía". (…)

Por tales motivos es muy importante que las empresas actúen de manera preventiva y no de manera a posteriori frente un posible incidente que ponga en riesgo la información recolectada (hecho superado), así mismo, cumplan con sus obligaciones como responsables o encargados de la información y, adopten los mecanismos de seguridad para evitar que se materialicen los incidentes que pongan en riesgo los datos personales de las personas y se eviten sanciones administrativas y pecuniarias por parte de la Superintendencia de Industria y Comercio, entidad que en el ejercicio de su facultad sancionatoria, en diferentes decisiones (Resolución N°3344 de 2020 y Resolución N°43704 del 2020) y en especial en la reciente resolución N°71984 proferida el 7 de julio de 2021 que las cita, es enfática en afirmar que:

"*La configuración de un hecho superado no significa que desaparezcan las eventuales irregularidades en que una empresa pudiera haber incurrido en el tratamiento de datos y no eximen de responsabilidad a quien haya cometido dichos errores. Por lo tanto, la SIC podrá iniciar la respectiva investigación administrativa de carácter sancionatorio contra quien, entre otras, alegue un hecho superado. Y se ha recalcado que ni la responsabilidad, ni la sanción frente a quien incumple el régimen jurídico de protección de Datos Personales se desvanece ante la configuración de un hecho superado"* (Resolución N°41984, 2021).

A dicha conclusión llegó la Superintendencia de Industria y Comercio, tras analizar en segunda instancia el caso de Avantel S.A.S. en reorganización, empresa que incumplió con la obligación contenida en el numeral 5 del artículo 8 de la ley 1266 de 2008, en el sentido de que no tenía autorización de la titular de la información para el tratamiento de los datos personales, y su argumento al momento de ejercer su derecho de defensa era que si bien no contaba con dicha autorización, ya había suprimido la información de la titular y la misma no se encontraba en las bases de datos de las centrales, situación que a su juicio constituía un "hecho superado". Con el agravante de que dicha empresa ya había sido sancionada anteriormente en diferentes procedimientos administrativos por otros hechos que pusieron en riesgo la información de los titulares, constituyéndose el criterio de graduación de la sanción establecido en el literal c del artículo 24 de la ley 1581 de 2021, en el sentido de que se trata de la denominada "reincidencia en la comisión de la infracción".

De lo anterior, se desprenden los riesgos que corren las empresas si no cumplen con la ley de Habeas Data, los cuales según José Guillermo Martínez (Martinez, 2017, págs. 70,71) son los de hacerse acreedoras a sanciones por parte de la SIC, ser objeto de multas por parte de la SIC hasta por 2.000 salarios mínimos legales mensuales vigente, la supresión de actividades relacionadas con el tratamiento de datos y, ser objeto de demandas por la responsabilidad civil que se pueda derivar del incumplimiento en el tratamiento de los datos personales.

Normas Corporativas Vinculantes

Recientemente el Ministerio de Industria, Comercio y Turismo en cumplimiento de lo establecido en el artículo 27 de la ley 1581 de 2012[3], publicó un proyecto de decreto mediante el cual se pretende establecer las condiciones mínimas para la elaboración de las Normas Corporativas Vinculantes, las garantías y mecanismos de protección de datos que deben ofrecerse y el procedimiento para autorizarlas.

La definición de Normas Corporativas vinculantes, la trae consigo el mismo proyecto de decreto de la siguiente manera:

(…) *"son Normas Corporativas Vinculantes las políticas o códigos de conducta de obligatorio cumplimiento asumidas por el responsable del tratamiento de datos, establecido en el territorio colombiano, para realizar transferencias o un conjunto de transferencias de datos personales a un responsable que se encuentre ubicado por fuera del territorio colombiano y que haga parte de un mismo grupo de empresas*" (…)

De igual manera, dentro de los requisitos generales que según el proyecto de decreto deben contener las normas Corporativas vinculantes, en otras palabras, se encuentran (i) la estructura y el contacto del grupo de empresas; (ii) las especificaciones de las transferencias de datos, el tipo de tratamiento y sus fines; (iii) su carácter jurídicamente

[3] El artículo 27 de la ley 1581 de 2012 dispuso que "el Gobierno Nacional Expedirá la reglamentación correspondiente sobre Normas Corporativas Vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países":

vinculante; (iv) la aplicación de los principios generales en materia de protección de datos personales; (v) la referencia de los derechos de los titulares; (vi) la aceptación de responsabilidad por parte del responsable en el territorio colombiano; (vii) las medidas adoptadas para evitar las transferencias a otras entidades; (viii) el personal encargado del cumplimiento de dichas normas; (ix) mecanismos para garantizar el cumplimiento de las Normas Corporativas Vinculantes; (x) mecanismos para comunicar las modificaciones de las precitadas normas; (xi) el mecanismo de cooperación con la Superintendencia de Industria y Comercio para garantizar el cumplimiento por parte del grupo de empresas; (xii) la formación en protección de datos para el personal con acceso a los mismos; (xiii) procedimientos para que los titulares presenten reclamos y consultas; (xiv) la adopción de medidas de responsabilidad demostrada y; (xv) las especificaciones o requisitos adicionales que haga la SIC.

Como su nombre lo indica, estas normas son jurídicamente vinculantes tanto interna como externamente por el mismo grupo de empresas responsables del tratamiento de los datos personales y como lo establece el proyecto de decreto, una vez diseñadas y aprobadas por los órganos competentes de las empresas deberán ser aprobadas por la Superintendencia de Industria y comercio, siempre y cuando cumplan los requisitos formales y materiales que se determinen para tal fin.

Si bien, pasaron casi 10 años desde que la ley 1581 de 2012 fue promulgada y ordenó al Gobierno la reglamentación de las Normas Corporativas Vinculantes, lo cierto es que son normas que se requerían con suma urgencia, teniendo en cuenta que con la

globalización, la apertura de los mercados, la inversión extranjera, la implementación del comercio electrónico y las nuevas tecnologías en la empresa, se puede presentar una mayor transferencia internacional de datos personales, poniendo en riesgo los derechos de los titulares de la información, por lo tanto, el objetivo de dichas normas es facilitar la transferencia de datos entre responsables que sean parte de un mismo grupo de empresas y que se encuentran ubicados en diferentes países.

Sin embargo, a mi parecer si se hubiesen reglamentado las Normas Corporativas Vinculantes inmediatamente después de promulgada la ley 1581 de 2012, las empresas como responsables del tratamiento de la información, hubiesen dispuesto todos sus esfuerzos para que al momento de cumplir con la reglamentación en materia de protección de datos personales, también diseñaran las normas corporativas vinculantes en caso de que le fueran aplicables, situación que les permitía ahorrar recursos técnicos, administrativos, humanos y financieros.

De igual manera, muchos inversionistas extranjeros que quieren ingresar al mercado colombiano con sucursales o fusionándose con otras sociedades, pueden ver al diseño de las Normas Corporativas Vinculantes como una barrera no arancelaria, poniendo en riesgo la inversión extranjera.

Conclusiones y recomendaciones

Como se puede evidenciar, la protección de los datos personales trae consigo múltiples obligaciones que deben cumplir las empresas como responsables de la información. Lastimosamente, es una ley que no ha tenido una suficiente pedagogía

que permita su aplicación en todos los sectores de la sociedad, sin embargo, debemos tener conciencia que el uso indebido de los datos personales e información que poseamos de terceras personas puede generar la vulneración a la intimidad, dignidad humana, el derecho a la honra, al buen nombre e incluso inducir al suicidio.

Es por esto que la protección de los datos personales en las empresas no es un juego, en este se ven involucrados los derechos de los titulares de la información, se encuentra comprometida su intimidad, su patrimonio, su honra, su buen nombre, por lo que se debe propender siempre por adoptar medidas de protección de la información, establecer políticas de protección acorde con sus necesidades y con que todo lo relacionado con el tratamiento de la información cumpla con la normatividad vigente, así como con los principios fundantes y rectores, que permiten un mayor entendimiento de cómo se debe realizar de manera adecuada la protección de los datos personales.

Por lo anterior, es recomendable que se revisen y se actualicen frecuentemente las políticas, que sean diseñadas con base en el objeto social de la empresa y los principios rectores de la protección de los datos personales, que cumplan con todos los estándares y recomendaciones de la Superintendencia de Industria y Comercio, también es necesario brindarle capacitación a sus empleados y contratistas sobre el manejo de datos sobre datos personales, realizar el registro de las bases de datos en el RNBD en el caso de que le corresponda dicha tarea, que se actualice el registro dentro del término y con base en las recomendaciones dadas por la entidad de protección de datos personales, que asimismo, se registren las nuevas bases de datos dentro de los 2 meses

siguientes a su creación. Aunado a lo anterior, en el evento de una filtración de la información o se presente una falla en las medidas de seguridad adoptadas, se informe dicha situación a la Superintendencia de Industria y Comerio y a los titulares, así como las medidas que fueron adoptadas dentro del término establecido por la entidad de protección de datos personales.

Seguro que si se siguen todas estas recomendaciones es probable que se reduzca el riesgo de un incumplimiento de la normatividad de datos personales que acarree sanciones pecuniarias y/o administrativas por parte de la Superintendencia de Industria y Comercio, entidad que entre septiembre de 2020 y agosto de 2021 impuso un total de 146 multas que ascienden a la cifra de $11.902.508.430, que en su gran mayoría fueron por quejas ciudadanas relacionadas con reportes a centrales de riesgos de información financiera por suplantación de identidad (Superintendencia de Industria y Comercio, 2021).

Una vez analizado el origen, la evolución, así como la normatividad aplicable a la protección de los datos personales, pasaré a estudiar cada uno de los principios rectores sobre esta materia, los cuales deben ser acatados por los responsables y encargados al momento de realizar el tratamiento de la información, evitando a toda costa la vulneración de los derechos de los titulares y reduciendo los riesgos de sanciones por parte de la Autoridad de Protección de Datos Personales.

11. PRINCIPIOS RECTORES DEL TRATAMIENTO DE LOS DATOS PERSONALES

Origen

Para realizar un análisis sobre los principios rectores del tratamiento de los datos personales en Colombia, es necesario remitirse inicialmente a lo señalado en el artículo 230 de la Constitución Política de 1991, que establece lo siguiente:

> *(…)* ***Artículo 230.*** *Los Jueces, en sus providencias, sólo están sometidos al imperio de la ley.*
>
> *La equidad, la jurisprudencia, los principios generales del derecho y la doctrina son criterios auxiliares de la actividad judicial" (…).*

Al respecto, la Corte Constitucional en la Sentencia C-284 de 2015 al estudiar una demanda de inconstitucionalidad frente al artículo 4 de la ley 153 de 1997 en la que se resaltó, entre otras cosas, que "*los principios de derecho natural y las reglas de jurisprudencia servirán para ilustrar la Constitución en casos dudosos"* (…); explicó que a los principios generales del derecho suelen atribuirse diferentes funciones dentro de la cuales se encuentran la función critica de los ordenamientos, en la que actúan como la imagen de un derecho ideal; otra función es la denominada "Integradora" en la que los principios actúan como verdaderas normas jurídicas, es decir, se activan a falta de ley de manera subsidiaria y, una última postura en la que se resalta que una de las tareas de los principios es precisar el alcance de las fuentes del derecho a lo que

denomina como función interpretativa, con el propósito de aclarar dudas o superar ambigüedades en las leyes. (Cconst, C-284/2015, M.González).

De igual manera, la precitada sentencia señala que los *"principios generales del derecho se encuentran subordinados a la ley y solo constituyen un criterio auxiliar de la actividad judicial. Ello implica que bajo ninguna circunstancia es posible, a la luz del artículo 230 de la carta, invocar un principio general del derecho con el objeto de derrotar o desplazar una norma jurídica vigente y que se encuentre comprendida por el concepto de ley.* (Cconst, C-284/2015, M.González).

Sin embargo, concluye la sentencia diciendo que cuando el principio sea incorporado mediante cualquier disposición en el ordenamiento jurídico, "*el enunciado correspondiente tendrá una nueva posición en el sistema de fuentes adquiriendo, si encuadra en el concepto de ley, la posición preferente que ésta ocupa según el artículo 230 de la carta política*", tal es el caso de los principios de protección de datos personales establecidos tanto en la ley 1266 de 2008 y ley 1581 de 2012 como lo pasaré a explicar más adelante.

Dada la importancia de los principios rectores al momento del tratamiento de los datos personales, se hace necesario hablar de ellos de manera detallada y específica en el presente acápite. Como primera medida, cuando hablamos de principios, debemos remitirnos a Robert Alexy quien los define como:

(…) "normas que ordenan que algo sea realizado en la mayor medida posible, dentro de las posibilidades jurídicas y reales existentes. Por lo tanto, los principios son mandatos de optimización, que se caracterizan porque pueden cumplirse en diferente grado, y que la medida debida de su cumplimiento no solo depende de las posibilidades reales sino también de los principios y reglas opuestos. En cambio, las reglas son normas que solo pueden ser cumplidas o no" (…) (Alexy, 2007, págs. 67-68)

Por su parte, en el artículo denominado El fundamento de los Principios Jurídicos: una cuestión problemática de José Julián Suárez, se hizo un estudio de la influencia que los principios jurídicos han tenido en el derecho constitucional colombiano y la manera como lo han transformado, desempeñando un papel preponderante en la tarea del juez a través de herramientas interpretativas para determinar los derechos y hacerlos efectivos. Adicionalmente, definió a los principios como *"enunciados normativos que contienen exigencias normativas derivadas de la dignidad humana y de la misma condición de persona".* (Suárez, 2016).

Para el desarrollo de su estudio, el precitado autor también se basó en la definición de principio que dio Dworkin considerándolo como un "*estándar normativo que ha de ser observado porque es una exigencia de la justicia, la equidad o alguna otra dimensión de Moralidad*" (Dworkin, 2010).

En el ámbito internacional, una de las primeras referencias fueron los denominados Principios rectores para la reglamentación de los ficheros computarizados de datos

personales, adoptados por la Asamblea General de la ONU mediante resolución 45/95 del 14 de diciembre de 1990, cuya aplicación se dio en los ficheros computarizados públicos o privados. Los principios aquí establecidos fueron los siguientes: 1) Principio de la Licitud y lealtad, 2) Principio de Exactitud, 3) Principio de Finalidad, 4) Principio de Acceso a la Persona Interesada, 5) Principio de no discriminación, 6) facultad de establecer excepciones, 7) Principio de Seguridad, 8) Control y Sanciones, 9) Flujo de datos a través de las fronteras, 10) Campo de Aplicación.

Al estudiar la materia en el ámbito interamericano, la Corte Constitucional resaltó que la Organización de los Estados Americanos OEA en el año 2010 expidió el documento denominado "Proyecto de principios y recomendaciones preliminares sobre la protección de datos". También, diseñó un catálogo de 15 directrices que definió como "*la base de la legislación sobre protección de datos en todo el mundo y que podrían servir de base para un instrumento internacional o una legislación modelo sobre protección de datos"* (Cconst, C-748/2011, J. Pretelt).

Principios Legales en Colombia

Por su parte, en Colombia la ley 1266 de 2008 que regula la protección de datos personales en materia crediticia, financiera y comercial, establece en su artículo 4 los siguientes principios para la administración de datos: a) Principio de Veracidad o calidad de los registros o datos, b) Principio de Finalidad, c)Principio de Circulación Restringida, d)Principio de Temporalidad, e) Principio de interpretación integral de derechos constitucionales, f) Principio de Seguridad, g) Principio de Confidencialidad.

Posteriormente, en el régimen general de protección de datos personales que trae consigo la ley 1581 de 2012, el artículo 4 establece que en relación con la interpretación y aplicación de precitada ley, se aplicarán de manera armónica e integral los siguientes principios:

a) Principio de Legalidad en materia de Tratamiento de Datos: El tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

Frente a este principio, las empresas que actúen como responsables o encargadas del tratamiento de los datos personales, deben desarrollar esta actividad cumpliendo fielmente sus deberes establecidos, respetando también los derechos de los titulares, obrando siempre de buena fe y cumpliendo con las disposiciones legales sobre la materia.

b) Principio de Finalidad: El tratamiento debe obedecer a una finalidad legítima de acuerdo con la constitución y la ley, la cual debe ser informada al Titular.

Sobre este principio, la Corte Constitucional al momento de estudiar su constitucionalidad señaló que la finalidad no sólo debe ser legítima sino que se destinará a realizar los fines exclusivos para la cual fue entregada y es por esto que se deberá informar al titular de manera *"clara, suficiente y previa acerca de la finalidad de la información suministrada y por tanto, no podrá recopilarse datos sin la clara especificación acerca de la finalidad de los mismos"* (Cconst, C-748/2011, J. Pretelt).

Claramente, los responsables del tratamiento deben definir cuál es esta finalidad y deberá informarla a los titulares de la información con el ánimo de que conozcan los usos que se le darán de manera específica a sus datos personales, esto permitirá a los titulares tomar una decisión informada y tener pleno control sobre su determinación de autorizar o no el tratamiento y las posibles consecuencias que esto implicaría. En todo caso, esto permitiría al titular verificar si efectivamente los responsables están realizando el tratamiento de los datos personales con base en las finalidades establecidas y en caso de que no sea así, tenga la facultad de ejercer sus derechos frente al responsable y frente a la Autoridad de Protección de Datos en los casos previstos en la ley.

La Corte Constitucional ha sido enfática en que este principio implique también un ámbito temporal, es decir, *"que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos"* (Cconst, C-748/2011, J. Pretelt), situación que impone a los responsables y encargados del tratamiento verificar sus bases de datos y depurarlas en la medida en que vayan cumpliendo su finalidad dentro del tiempo previsto. De igual manera, esto es importante a la hora de actualizar su información en el Registro Nacional de Base de Datos administrado por la Superintendencia de Industria y Comercio.

c) Principio de Libertad: El tratamiento sólo puede ejercerse con el consentimiento, previo expreso e informado del titular. Los datos personales no podrán

ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento.

Este principio, por un lado otorga la facultad a los titulares de autorizar o no el tratamiento de su información de manera libre, informada y espontánea y, por otro lado, impone la obligación a los responsables y encargados de contar siempre con autorización por parte de los titulares para el tratamiento de los datos personales que son almacenados en sus bases de datos, conservando dicha autorización de tal manera que pueda ser consultada en cualquier momento por el titular, sus causahabientes y/o por la autoridad de protección de datos personales.

En relación con las características del consentimiento, cuando nos referimos a previo, quiere decir que antes de realizar el tratamiento de los datos personales, el titular debe autorizar a los responsables para realizar dicha operación y usar su información, de lo contrario estaríamos frente a una vulneración del derecho al habeas data, salvo que estemos frente a una excepción legal o se trate de una orden judicial motivada.

En cuanto al carácter expreso del consentimiento, la Corte Constitucional ha resaltado que en el ordenamiento jurídico colombiano, no es posible la existencia de un consentimiento tácito, ya que debe ser explícito y concreto a la finalidad de la base de datos. Para la corte, al hacer una interpretación armónica de este principio y de los demás apartes de la ley general de protección de datos, se puede deducir que *"el legislador estatutario tuvo una intención inequívoca que el consentimiento siempre fuese expreso*" (Cconst, C-748/2011, J. Pretelt), máxime aún que el responsable del

tratamiento tiene como deber el garantizar al titular el derecho de solicitar prueba de la autorización. Adicionalmente, la ley en su artículo 9 que detalla la autorización del titular, se establece que esta debe ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

Por último, el carácter informado implica que el titular al momento de otorgar la autorización en ejercicio de su voluntad libre y espontánea tiene que conocer la finalidad del tratamiento y poder hacerse la idea de la consecuencias e implicaciones que tiene el almacenamiento y uso de sus datos personales por parte del responsable.

d) Principio de Veracidad o calidad: la información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

e) Principio de Transparencia: en el tratamiento debe garantizarse el derecho del titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Este principio es importante para que el titular pueda ejercer de manera efectiva sus derechos a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, establecidos en la ley general de protección de datos personales. Permite que el titular tenga claro el panorama acerca de que información tiene determinado responsable del tratamiento y en caso de que no sea

veraz solicite su rectificación, en caso de que sea incorrecta solicite su corrección y en caso de que considere que han sido vulnerados sus derechos o se ha cumplido con el ámbito temporal de la finalidad establecida, solicite su supresión.

La Corte Constitucional al estudiar este principio, determinó que el Responsable o el encargado del tratamiento de la información, debe ofrecer como mínimo al titular:

> *(…) i) información sobre la identidad del controlador de datos, (ii) el propósito del procesamiento de los datos personales, iii) a quien se podrán revelar los datos, iv) cómo la persona afectada puede ejercer cualquier derecho que le otorgue la legislación sobre protección de datos; y v) toda otra información necesaria para el justo procesamiento de los datos" (..) (Cconst, C-748/2011, J. Pretelt)*

f) Principio de Acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley.

Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, a no ser que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la presente ley.

g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá

manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

De acuerdo con los dos principios anteriores, le corresponde a los responsables o encargados del tratamiento de los datos personales, adoptar medidas administrativas y técnicas que sean robustas para garantizar la efectiva seguridad y conservación de la información suministrada por los titulares, para evitar y minimizar los riesgos de filtraciones que puedan generarle a estos últimos perjuicios graves en su privacidad, intimidad, honra y buen nombre, lo que podría constituirse como una vulneración al derecho fundamental del habeas data.

Cabe resaltar que en caso de que se presente alguna filtración de la información que ponga en riesgo la intimidad y el derecho del habeas data a los titulares, el responsable o encargado deberán notificar dentro de los términos legales a la autoridad de protección de datos personales así como a los titulares mismos, explicando las medidas adoptadas para el resarcimiento de la situación y las medidas que se van a adoptar con posterioridad a la filtración para evitar que ocurra nuevamente, esto además, es una causal de atenuación al momento de la tasación de la sanción pecuniaria que se encuentra en cabeza de la autoridad de protección de datos personales.

h) Principio de Confidencialidad: todas las personas que intervengan en el Tratamiento de Datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su

relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley en los términos de la misma.

En este punto cabe recalcar la importancia de que el principio de seguridad y confidencialidad vayan de la mano, ya que el uno depende del otro. Las medidas de seguridad implican la confidencialidad de todas las personas que intervienen en el tratamiento de los datos personales. Por eso siempre se recomienda el diseño y cumplimiento de las políticas de privacidad, que en los contratos que celebren los responsables y encargados siempre se establezcan cláusulas de protección de datos personales y acuerdos de confidencialidad que en caso de incumplimiento se derive en la cláusula penal.

Dichos principios, revisten de tal importancia que incluso deben ser aplicados a las bases de datos que son exceptuadas del régimen general de protección de datos personales como lo son las del ámbito personal o doméstico, a las que tengan por finalidad la seguridad y defensa nacional, a las de información de inteligencia y contrainteligencia, a las de información periodística y otros contenidos editoriales, a las reguladas por la ley 1266 de 2008 (régimen de protección de datos personales financieros, crediticios y comerciales) y las reguladas por la ley 79 de 1993 (Censos).

Sin embargo, tal y como lo estableció la Corte Constitucional al estudiar la constitucionalidad de la ley general de protección de datos personales, *"debe entenderse que la enunciación de estos principios no puede entenderse como la*

negación de otros que integren o lleguen a integrar el contenido del derecho fundamental" (Cconst, C-748/2011, J. Pretelt). Tal disposición es importante en la medida en que con el paso del tiempo y los avances legales, doctrinales y jurisprudenciales pueden establecerse unos nuevos principios que permitan garantizar de manera más amplia el derecho de habeas data.

De igual manera, la Corte Constitucional en la precitada sentencia, resaltó una serie de principios que a su parecer se entienden incluidos dentro de la ley general de protección de datos personales, como serían los derivados directamente de la constitución: i) prohibición de discriminación, ii) principio de interpretación integral de los derechos constitucionales y iii) obligación de indemnizar los perjuicios. También, los denominados principios derivados del núcleo temático del proyecto de ley estatutaria: i) principio de la proporcionalidad del establecimiento de excepciones, ii) principio de autoridad independiente, iii) principio de exigencia de estándares de protección equivalentes para la transferencia internacional de datos. Para la Corte constitucional estos principios *"deben entenderse de manera armónica, coordinada y sistemática respetando en todo caso los contenidos básicos del derecho fundamental del habeas data"* (Cconst, C-748/2011, J. Pretelt).

Principios actualizados del Comité Jurídico Interamericano sobre la privacidad y la protección de datos personales con anotaciones.

Teniendo en cuenta que la enunciación de los principios que trae consigo la ley 1581 de 2012, no puede entenderse como la negación de otros que lleguen a integrar el

contenido del derecho del habeas data, pasaré a realizar un análisis de los principios actualizados recientemente por el Comité Jurídico Interamericano (CJI) sobre la Privacidad y la Protección de datos personales de la Organización de los Estados Americanos OEA, cuya finalidad es *"contribuir al desarrollo de un marco vigente para salvaguardar los derechos de la persona a la protección de sus datos personales y a la autodeterminación en lo que respecta a la información en los países de las Américas"* (Comité Jurídico Interamericano CJI de la Organización de los Estados Americanos, 2021).

La actualización de los principios según la CJI se basó en las normas y estándares reconocidos internacionalmente hasta el año 2020, con el ánimo de proteger los derechos de las personas sobre el tratamiento de sus datos personales. Su finalidad, es guiar a los Estados Miembros de la OEA para el fortalecimiento de sus normas sobre la protección de los datos personales, para que los mismos determinen cual es la mejor manera de tener en cuenta estos principios dentro de su ordenamiento jurídico. Los principios estudiados, buscan proporcionar elementos para una protección efectiva del derecho de habeas data, en palabras de la CJI: *"reflejan la importancia, la razonabilidad, la proporcionalidad y la flexibilidad como elementos rectores".*

a) Principio de Finalidades Legítimas y lealtad

Según el informe del CJI la recopilación de datos personales debería ser limitada y realizarse con el conocimiento o el consentimiento de la persona. Afirma que no deberían recopilarse datos sobre personas excepto en las situaciones y con los métodos

permitidos o autorizados por ley. El requisito de legitimidad comprende el concepto de legalidad y excluye el tratamiento arbitrario de datos personales.

Este principio, implica dar a conocer claramente a los titulares al momento de la recolección de los datos personales, acerca de las finalidades del tratamiento, con la finalidad de que conozcan y entiendan como se usarán y trataran sus datos.

En relación con los medios legales y legítimos que trae este principio, se requiere que los medios empleados para la recolección de los datos personales sean compatibles tanto con los requisitos legales como con las expectativas basadas en el vínculo que se tiene con los responsables del tratamiento de la información. Excluye la recolección de datos por medio de fraude.

b) Principio de Transparencia y Consentimiento

En cuanto al principio de transparencia en materia de protección de datos personales, el informe establece que, al momento de recopilarse la información, se deben especificar de manera clara:

(...) ***i)*** *la identidad y datos de contacto del responsable;* ***ii)*** *las finalidades del tratamiento;* ***iii)*** *el fundamento jurídico de su tratamiento;* ***iv)*** *los destinatarios o categorías de destinatarios a los cuales los datos personales serán comunicados;* ***v)*** *la información a serles transmitida;* ***vi)*** *la existencia, forma y mecanismos o procedimientos a través de los cuales los Titulares de Datos Personales podrán ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad" (...)*

(Comité Jurídico Interamericano CJI de la Organización de los Estados Americanos, 2021)

Lo anterior, con la finalidad de informar a las personas sobre las políticas de los responsables o encargados del tratamiento de la información, para tomar una decisión fundamentada al momento de entregar los datos personales.

De igual manera, las personas titulares deberán dar su consentimiento de manera libre y voluntaria, basado en la suficiente información sobre los detalles de los datos que serán recopilados y las finalidades de su tratamiento, evitando la coacción y engaño por parte de los responsables o encargados.

c) Principio de Pertinencia y necesidad

Son principios indispensables para el tratamiento de la información, imponen limitaciones para que los datos personales solo sean usados para el cumplimiento de los propósitos de la recopilación. Sin embargo, con la actualización del informe de la CJI se abrió la posibilidad para que en una medida razonable fueran más flexibles y adaptables, debido a la evolución continúa de las nuevas tecnologías.

Estos principios establecen unos límites para proteger la información de lo titulares, ya que obliga a los responsables o encargados a tratar los datos única y exclusivamente para las finalidades solicitadas y autorizadas, sin embargo, en muchas ocasiones vemos como en los formatos de autorización de uso y tratamiento de datos confeccionados por las empresas, se ponen una gran cantidad de finalidades, lo que puede generar que

el uso de la información permanezca en el tiempo y sea más implícita, situación que también pone en riesgo la privacidad y los derechos de los titulares. Es por esto, que las empresas deben adaptar los consentimientos de los titulares a las finalidades específicas, es decir, si los datos recopilados son para determinado evento, una vez este sea culminado se recomienda que la empresa suprima la información o se abstenga de realizarle tratamiento a la misma, no obstante la anterior, tal y como se ha explicado a lo largo del presente estudio, las empresas viven de los datos personales de sus clientes y consumidores y las nuevas tecnologías permiten su masificación.

d) Principio de tratamiento y conservación limitados

Este principio, tiene una estrecha relación con el anteriormente explicado, teniendo en cuenta el tiempo en el que se deben conservar los datos personales por los encargados y responsables del tratamiento. El informe del CJI es enfático en afirmar que una conservación que no sea necesaria y que sea excesiva genera implicaciones en la privacidad de los titulares, argumentando que una de sus causales es la reducción en el costo del almacenamiento de la información a favor de los responsables y los encargados, situación que genera que estos no se preocupen por hacer un análisis para determinar cuáles datos no se están utilizando con el ánimo de suprimirlos. Por lo tanto, los responsables deben adaptar procedimientos para eliminar de manera segura y definitiva los datos que se encuentren en sus bases tanto electrónicas como físicas o someterlos a un proceso de anonimización para fines estadísticos o contables con un interés público o legal, casos en los cuales pueden conservarse durante períodos con

una mayor duración, siempre en cumplimiento del principio de responsabilidad demostrada con medidas de seguridad y administrativas robustas que garanticen el derecho de los titulares.

e) Principio de Confidencialidad

El principio de confidencialidad en materia de protección de datos personales, impone la obligación a los responsables y encargados de mantener la información en un entorno seguro y controlado, con la finalidad de que no se divulguen ni se pongan a disposición de terceros, generando riesgo la privacidad y a los derechos de los titulares, salvo que se cuente con el consentimiento previo por estos últimos o en los casos previstos en la ley, generando confianza en los intervinientes durante el ciclo del tratamiento de la información.

f) Principio de seguridad de los datos.

Este principio tiene un vínculo estrecho e inseparable con el principio de confidencialidad, pues de las medidas de seguridad técnicas, administrativas u organizacionales que adopten los encargados y responsables del tratamiento, depende la adecuada confidencialidad de la información, evitando su filtración y la vulneración de los derechos de los titulares.

Según el informe del CJI las medidas para proteger los datos personales deben ser elegidas o adoptadas por los responsables o encargados teniendo en cuenta los siguientes factores: *(i) "la posible afectación a los derechos de los titulares, en particular, el posible valor de los datos para una tercera persona no autorizada para*

su tratamiento; (ii) los costos de su implementación; (iii) las finalidades del tratamiento y; (iv) la naturaleza de los datos personales tratados, en especial los datos sensibles" (Comité Jurídico Interamericano CJI de la Organización de los Estados Americanos, 2021).

Según la actualización de los principios dada por este informe, en el contexto moderno, es imposible la privacidad absoluta y protección de los datos personales, ya que para lograrlo existen barreras costosas e inaceptables para los responsables, por lo que en estos casos se deberá realizar una valoración razonada e informada ya que cualquier acceso no autorizado no siempre constituye una vulneración de la privacidad. A mi juicio, esta última afirmación pretende ser más flexible con los responsables y encargados del tratamiento, dejando a un lado la finalidad específica y el objeto del régimen de protección de datos personales y en cierta medida traslada la responsabilidad a los titulares para que decidan qué información quieren entregar y a quien se la quieren dar.

En este sentido, se requiere que con el devenir del tiempo, con los avances tecnológicos y la evolución de las amenazas a la privacidad, sean revisadas, evaluadas y actualizadas las medidas de seguridad adoptadas por los responsables y encargados del tratamiento.

g) Principio de Exactitud de los Datos

Según el informe del CJI la exactitud y la precisión son vitales para la protección de la privacidad, teniendo en cuenta que los datos que tengan la naturaleza de inexactos

perjudican tanto a los responsables como a los titulares. Por un lado, los responsables durante la conservación y almacenamiento de la información tienen la obligación de que los datos se mantengan actualizados para no alterar su veracidad, para el cumplimiento de la finalidad para la cual fueron recolectados, por lo tanto, se recomienda disponer recursos técnicos y administrativos para darle la oportunidad a los titulares para actualizar sus datos personales o para que soliciten su supresión y también, para eliminar a mutuo propio los datos que ya cumplieron su finalidad.

h) Principio de Acceso, rectificación, cancelación, oposición y portabilidad

Este principio de que trata el informe del CJI analiza básicamente los derechos que tienen los titulares de la información frente a los datos personales tratados por los responsables o encargados.

En relación con el acceso, es ese derecho que tenemos las personas para conocer si determinado responsable tiene información relacionada con nosotros y en caso de que así sea, poder conocer cual se encuentra almacenada. En palabras de la CJI este debería ser un derecho sencillo de ejercer, debe ser parte de las actividades que realice regularmente el responsable del tratamiento y no se debería solicitar alguna medida especial, costo o procedimiento judicial para tal fin.

En cuanto con la rectificación, las personas tenemos derecho a solicitarle a los responsables o encargados que se revisen, se corrijan o eliminen los datos personales almacenados. También a que los datos personales sean cancelados, a hacer objeciones frente al tratamiento y a su portabilidad en los casos previstos.

En el informe del CJI se establece enfáticamente que los países miembros de la OEA, deberán fijar los plazos, términos y condiciones para que los titulares puedan ejercer los derechos así como las excepciones sobre los mismos. En el caso de Colombia, estos términos y condiciones se encuentran establecidos en el régimen general de la protección de los datos personales (ley 1581 de 2012). Estos, también son establecidos según su misionalidad, recursos técnicos y administrativos en las Políticas de Privacidad adoptadas por los Responsables y encargados del tratamiento.

Cuando se habla del derecho de portabilidad, estamos hablando acerca de la posibilidad que tienen los titulares para obtener una copia en un formato electrónico de sus datos personales, que permita seguir usándolos y transferirlos a otro responsable sin impedimento alguno. Este es un derecho que según el informe del CJI, continúa siendo discutido interiormente por los estas miembros de la OEA.

i) Principio de Datos Personales Sensibles

Para el CJI los estados miembros de la OEA deben establecer en su legislación la categoría de datos personales sensibles, teniendo en cuenta que merecen protección especial ya que su manejo inadecuado da lugar a desencadenar una discriminación arbitraria contra las personas y causarles graves perjuicios. Estos datos pueden estar relacionados con la salud, orientación y vida sexual, orientación política y religiosa, datos biométricos, afiliación a sindicatos y datos genéticos. El informe señala que en principio esta categoría de datos no debe ser tratados, salvo que el titular de autorización explícita y su tratamiento sea estrictamente necesario.

Por lo tanto, los responsables y encargados deben evitar al máximo el tratamiento de los datos sensibles, pero en el evento en que se requieran para la finalidad última como lo sería para el cumplimiento de un mandato legal, salvaguarda de derechos del titular o de terceros o para efectos de seguridad nacional o salud pública, se deberán tomar medidas de protección para la seguridad y confidencialidad de los mismos, con la intención de evitar graves perjuicios a los titulares que se deriven en discriminaciones de diversa índole.

j) Principio de Responsabilidad

En el informe objeto de estudio, el principio de responsabilidad se encuentra relacionado con el establecimiento de medidas más apropiadas para alcanzar las metas y vigilar su cumplimiento por parte de los responsables de datos personales, acordes con su estructura administrativa, tamaño empresarial y sus recursos.

En la presente investigación, estudiaremos de manera detallada este principio ya que es considerado uno de los más importantes para garantizar la confidencialidad de la información con medidas de seguridad robustas que permita salvaguardar íntegramente los derechos de los titulares.

En cuanto la actualización de este principio que realiza la CJI, se encuentra basada en el enfoque contemporáneo consistente en que los responsables de datos incorporen la protección de la privacidad en el diseño de sus sistemas tecnológicos y en sus prácticas empresariales, desde antes de la recopilación de los datos para identificar los riesgos inherentes al tratamiento de la información.

k) Principio de Flujo transfronterizo de datos y responsabilidad

El informe reconoce un valor especial que tiene para el desarrollo económico y social el flujo transfronterizo de datos, por lo que considera que los estados miembros deben cooperar para facilitar dicho flujo siempre y cuando los estados garanticen un nivel adecuado de protección de datos.

Esta transferencia transfronteriza ha tenido una mayor acogida con ocasión a como lo hemos venido manifestando a lo largo de esta investigación, principalmente por la globalización, la apertura de los mercados y la implementación de las nuevas tecnologías en el comercio. Sin embargo, en muchos estados la regulación del tratamiento de la información no es adecuada para garantizar efectivamente los derechos de los titulares, situación que pone en riesgo su privacidad y abre la posibilidad de generar daños y perjuicios que afecten su proyecto de vida.

Para la CJI el reto consiste en conciliar *1) "las diferencias en los enfoques nacionales de la protección de la privacidad con la realidad moderna del flujo mundial de datos, 2) los derechos de las personas a tener acceso a datos en un contexto trasnacional; y 3) el hecho fundamental de que los datos y el tratamiento de datos impulsan el desarrollo y la innovación"* (Comité Jurídico Interamericano CJI de la Organización de los Estados Americanos, 2021)

En ese sentido, los estados deben evaluar si su normatividad es la adecuada para garantizar los derechos de los titulares cuando sus datos sean transferidos de otros

países y debe verificar a cuáles países se recomienda su transferencia, en pro del bienestar de sus ciudadanos, exigiendo siempre que los responsables de datos tomen medidas razonables para la protección eficaz de la información. Para tal fin, se requiere una cooperación entre los estados miembros para el reconocimiento de las reglas para evitar conflictos en la materia y resolverlos cuando surjan.

l) Principio de Excepciones.

Este principio se encuentra encaminado en garantizar que cualquier excepción debe encontrarse establecida taxativamente en la legislación de los estados, para que sean conocidas por las personas intervinientes en el tratamiento y se encuentran limitados a temas específicos como la seguridad nacional, la salud y el interés públicos.

Como lo hemos mencionado, no todos los derechos son absolutos, hay muchos que entran en constante colisión y es ahí donde se debe ponderar acerca de cuál debe tener una mayor protección teniendo en cuenta el caso específico. Todas las libertades tienen una limitación y le corresponde al legislador en el ejercicio de sus funciones establecer cuáles son esas excepciones y en qué casos son aplicables, después de hacer un análisis exhaustivo acerca de la dignidad, el honor y demás derechos fundamentales de las personas.

m) Principio de autoridades de protección de datos personales.

Según el informe cada estado miembro de la OEA deberá abordar individualmente la estructura, funciones y naturaleza de las Autoridades Responsables de la Protección de Datos, dotándolos de capacidad de cooperación internacional relacionadas con la

protección de datos. Adicionalmente, deberían establecer sanciones y recursos para los casos de incumplimiento en materia de protección de datos personales.

En el caso colombiano, la autoridad de protección de datos es la Superintendencia de Industria y Comercio a través de la Delegatura de Protección de Datos, entidad adscrita al gobierno nacional y la cual cumple funciones administrativas sancionatorias en caso de incumplimiento y que a lo largo de su historia ha sancionado drásticamente a los responsables que han incumplido con sus obligaciones y puesto en riesgo los derechos de los titulares. También, ha sido una entidad que ha realizado documentos, investigaciones y guías para asesorar y hacerle recomendaciones a los responsables y encargados con el ánimo de garantizar una protección efectiva de los derechos y minimizar los riesgos inherentes al tratamiento.

Como lo vimos anteriormente, la Superintendencia de Industria y Comercio ha sido víctima de muchas críticas justificadas, relacionadas con su independencia debido a que hace parte de la rama ejecutiva.

En conclusión, el informe del Comité Jurídico Interamericano de la Organización de los Estados Americanos, presenta una actualización de los principios inherentes a la protección de datos personales, necesaria para que los Estados Miembros de la OEA, los responsables y encargados del tratamiento que los integran, adecuen su normativa, sus políticas de protección para garantizar que se encuentren acorde con la situación fáctica y a los avances tecnológicos, la globalización y la apertura de los mercados, espacios en los cuales son de vital importancia y transcendencia los datos personales

almacenados en sus bases de datos de los clientes, proveedores, aliados estratégicos, trabajadores, contratistas, consumidores, entre otros.

Ahora bien, habiendo realizado un análisis del origen, características y normatividad aplicable al tratamiento de los datos personales en Colombia, pasaremos a estudiar el origen y normativa del comercio electrónico, dado el vínculo estrecho e inseparable entre estos dos temas, con ocasión a la globalización y el crecimiento exponencial de la comercialización de productos a través del E-commerce, dejando a un lado las ventas tradicionales, situación que lleva consigo la recolección masiva de información personal de los consumidores, ya que como lo dijo Pedro Pablo Camargo (Camargo, El Habeas Data , 2013, pág. 201) es bien sabido que los progresos e innovaciones tecnológicas presentadas en las dos últimas décadas han puesto a disposición de la humanidad nuevos medios de intercambio y de comunicación de la información. Para posteriormente vincular este tema con el principio de responsabilidad demostrada y conclusiones y recomendaciones acerca del objeto de estudio de la investigación.

12. EL COMERCIO ELECTRÓNICO EN COLOMBIA

Marco conceptual

Las nuevas tecnologías han generado que las empresas cambien sus estrategias de negocios, con el ánimo de llegar a una mayor cantidad de clientes, ingresar a un mercado más amplio en igualdad de condiciones, interactuar con personas a nivel mundial y han reducido el costo de las transacciones entre los empresarios. Las TIC´s permiten que los empresarios mediante mensajes de datos puedan comercializar y

ofrecer sus productos a través del comercio electrónico, generando una relación que beneficia mutuamente a clientes y comerciantes. Por una parte, los clientes no tienen que desplazarse a los establecimientos de comercio y puede adquirir una gama de productos desde cualquier lugar del mundo y a cualquier hora del día. Por otro lado, permite que las empresas ingresen a nuevos mercados y sus productos o servicios llegue a una mayor cantidad de consumidores.

El no uso de estas nuevas tecnologías por parte de las empresas, pueden acarrear graves perjuicios económicos ya que perderían muchas oportunidades de negocios frente a otras empresas que si las tengan implementadas y ofrezcan sus productos a precios más bajos. Es por esto, que el Comercio Electrónico permite a las empresas competir en un mercado mucho más global y accesible, pudiendo generar mayores ingresos y rentabilidad en sus negocios.

No obstante lo anterior, no basta que las empresas establezcan mecanismos para la implementación de las nuevas tecnologías en el giro ordinario de sus negocios y cumplan con la normatividad que es aplicable, sino que requieren generar confianza y seguridad en los consumidores para que adquieran los productos a través de las plataformas electrónicas dispuestas, ya que la desconfianza, los límites en el acceso y desconocimiento del funcionamiento de las TIC´s es el mayor obstáculo que se presenta al momento de su implementación. Adicionalmente, la implementación de las nuevas tecnologías requiere que el Internet sea accesible para todos, es por esto que el Comercio Electrónico ha tenido una mayor acogida en países donde el nivel de

conectividad es mayor que en países en los cuales la mayor parte de su población no puede acceder a estas plataformas.

Ahora bien, dentro de las definiciones dadas por algunos doctrinantes sobre el Comercio electrónico, podemos encontrar las siguientes:

Para la Doctrinante Gladys Stella Rodríguez el Comercio electrónico *"es entendido como la venta y compra directa o indirecta de cualquier tipo de información, productos y servicios por medio de redes de computadoras, así como también, el apoyo brindado a cualquier tipo de Transacción de negocios sobre una infraestructura digital"* (Rodríguez, 2001).

Otra definición es la que da Osío, citada por la autora nombrada anteriormente (Rodríguez, 2001), que considera al Comercio electrónico como *"la actividad de adquirir o enajenar a través de medios electrónicos bienes corporales o incorporales".*

En cuanto a sus generalidades, el literal b del artículo 2 de la ley 527 de 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*", define al comercio electrónico de la siguiente manera:

> *(...) "b) Comercio Electrónico. Abarca las cuestiones suscitadas por toda 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 medio similar. Las*

relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios, todo acuerdo de distribución, toda operación de representación o mandato comercial, todo tipo de operaciones financieras, bursátiles y de seguros, de construcción de obras, de consultoría, de ingeniería, de concesión de licencias, todo acuerdo de concesión o de explotación de un servicio público, de empresa conjunta y otras formas de cooperación industrial o comercial, de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea o por carretera" (...).

Por lo tanto, los empresarios para llevar a cabo las actividades que abarca la definición del Comercio Electrónico, requieren diseñar un sitio de internet (página web) donde den a conocer sus productos y la información que considere necesaria para atraer a los consumidores de sus bienes y servicios. Al respecto, el artículo 8 del decreto 3512 de 2003, define sitio de internet como:

"*El conjunto de elementos computacionales que permiten el almacenamiento, intercambio y/o distribución de contenidos en formato electrónico a los que se puede acceder a través de Internet o de cualquier otra red de comunicaciones y que se disponen con el objeto de permitir el acceso al público o a un grupo determinado de usuarios. Incluye elementos computacionales que permiten, entre otros servicios, la distribución o intercambio de textos, imágenes, sonidos o videos".*

Si bien, el sitio de internet y la página web no se encuentran dentro de la definición y los elementos integrantes de establecimiento de comercio que traen consigo el artículo 15 y el artículo 16 del Código de Comercio, la doctrina ha considerado que:

> *"El sitio de internet o la página web puede ser parte del establecimiento de los empresarios que operan de manera simultánea tanto en la internet, como en el medio físico a través de mecanismos tradicionales. Pero, cuando éstos son los únicos bienes que tiene el empresario para realizar los fines de la empresa, dicho sitio o página web constituyen el establecimiento de comercio del empresario"* (Remolina, 2006).

Es pues una tarea que tiene el empresario para determinar si el sitio de internet o página web hacen parte o constituyen el establecimiento de comercio, de acuerdo con sus necesidades y, con base en ello, diseñarlo e implementarlo conforme con su objeto social.

Protección al Consumidor de Comercio Electrónico

En cuanto a los consumidores de los productos de las diferentes empresas que han decidido implementar el comercio electrónico, dada la asimetría entre ellos con los productores o proveedores de bienes y servicios, se requiere que los últimos cumplan con todas y cada una de obligaciones (que son de orden público y de naturaleza imperativa) establecidas en el capítulo denominado "Protección al consumidor de Comercio electrónico" establecido en la ley 1480 de 2011, sin perjuicio de los derechos de los consumidores establecidos en la misma normatividad, situación que permitirá a

los empresarios generar un mayor grado de confianza y seguridad al momento de la transacción electrónica, evitando a toda costa la comisión de prácticas comerciales desleales, fraudes o engaños que afecte el Godwill de la compañía. Al respecto, para explicar la importancia y la relación existente entre la seguridad y confianza que brinda el comercio electrónico, la doctrina ha señalado que:

> "*en esta materia es crucial que el empresario periódicamente revise los mecanismos y estrategias de seguridad (tecnológicas, humanas, organizacionales, porque lo que es confiable hoy, de pronto no lo sea mañana. La "Confiabilidad", por su parte, normalmente guarda relación con el buen funcionamiento de los mecanismos de seguridad"* (Maria Lorena Florez, 2012).

Aquí, juega un papel preponderante la información de los productos o servicios suministrada por los empresarios, en el sentido de que debe ser veraz, completa y comprensible, para que al momento de tomar las decisiones conozca de manera detallada la calidad, las características subjetivas y objetivas de los mismos, conozca cómo será la transacción electrónica, los envíos, las garantías, los derechos que se tienen, así como los demás términos y condiciones establecidos por los comerciantes. De igual manera, es importante que los consumidores conozcan cuales son los datos personales que son tratados con ocasión de la negociación, cuáles son sus derechos y como los pueden hacer efectivos con base en la política de privacidad establecida por los proveedores y productores de los bienes y servicios.

El deber de información se encuentra estrechamente vinculado con la publicidad de los bienes y servicios ofrecidos por las empresas, entre más clara y veraz la información, se reduce el riesgo de emitir publicidad engañosa, la cual se encuentra definida como *"aquella cuyo mensaje no corresponda a la realidad o sea insuficiente, de manera que induzca o pueda inducir a error, engaño o confusión*[4]*"*

Pero no solo es ese deber de información el que tienen los proveedores que hayan decidido implementar el comercio electrónico en el giro ordinario de sus negocios, sino que además deben tener en cuenta las siguientes obligaciones establecidas en el artículo 50 de la ley 1480 de 2011:

a) *Informar en todo momento de forma cierta, fidedigna, suficiente, clara, accesible y actualizada su identidad especificando su nombre o razón social, Número de identificación tributaria (NIT), dirección de notificación juridicial, teléfono, correo electrónico y demás datos de contacto.*
b) *Suministrar en todo momento información cierta, fidedigna, suficiente, clara y actualizada, respecto de los productos que ofrezcan. En especial, deberán indicar sus características y propiedades tales como el tamaño, el peso, la medida, el material del que está fabricado, su naturaleza, el origen, el modo de fabricación, los componentes, los usos, la forma de empleo, las*

[4] Numeral 13 del artículo 5 de la ley 1480 de 2011.

propiedades, la calidad, la idoneidad, la cantidad, o cualquier otro factor pertinente, independientemente que se acompañen de imágenes, de tal forma que el consumidor pueda hacerse una representación lo más aproximada a la realidad del producto. También se deberá indicar el plazo de validez de la oferta y la disponibilidad del producto, en los contratos de tracto sucesivo, se deberá informar su duración mínima. Cuando la publicidad del bien incluya imágenes o gráficos del mismo, se deberá indicar en qué escala está elaborada dicha representación.

c) *Informar, en el medio de comercio electrónico utilizado, los medios que disponen para realizar los pagos, el tiempo de entrega del bien o la prestación del servicio, el derecho de retracto que le asiste al consumidor y el procedimiento para ejercerlo, y cualquier otra información relevante para que el consumidor pueda adoptar una decisión de compra libremente y sin ser inducido en error. Igualmente deberá informar el precio total del producto incluyendo todos los impuestos, costos y gastos que deba pagar el consumidor para adquirirlo. En caso de ser procedente, se debe informar adecuadamente y por separado los gastos de envío.*

d) *Publicar en el mismo medio y en todo momento, las condiciones generales de sus contratos, que sean fácilmente accesibles y disponibles para su consulta, impresión y descarga, antes y después de realizada la transacción, así no se haya expresado la intención de contratar. Previamente a la finalización o terminación de cualquier transacción de*

comercio electrónico, el proveedor o expendedor deberá presentar al consumidor un resumen del pedido de todos los bienes que pretende adquirir con su descripción completa, el precio individual de cada uno de ellos, el precio total de los bienes o servicios y, de ser aplicable, los costos y gastos adicionales que deba pagar por envío o por cualquier otro concepto y la sumatoria total que deba cancelar. Este resumen tiene como fin que el consumidor pueda verificar que la operación refleje su intención de adquisición de los productos o servicios ofrecidos y las demás condiciones, y de ser su deseo, hacer las correcciones que considere necesarias o la cancelación de la transacción. Este resumen, deberá estar disponible para su impresión o descarga.

La aceptación de la transacción por parte del consumidor deberá ser expresa inequívoca y verificable por la autoridad competente. El consumidor debe tener el derecho de cancelar la transacción hasta antes de concluirla.

Concluida la transacción, el proveedor y expendedor deberá remitir, a más tardar el día calendario siguiente de efectuado el pedido, un acuse de recibo del mismo, con información precisa del tiempo de entrega, precio exacto incluyendo los impuestos, gastos de envío y la forma en que se realizó el pago.

Queda prohibida cualquier disposición contractual en la que se presuma la voluntad del consumidor o que su silencio se considere como

consentimiento, cuando de esta se deriven erogaciones u obligaciones a su cargo.

e) Mantener en mecanismos de soporte duradero la prueba de la relación comercial, en especial de la identidad plena del consumidor, su voluntad expresa de contratar, de la forma en que se realizó el pago y la entrega real y efectiva de los bienes o servicios adquiridos, de tal forma que garantice la integridad y autenticidad de la información y que sea verificable por la autoridad competente, por el mismo tiempo que se deben guardar los documentos de comercio.

f) Adoptar mecanismos de seguridad apropiados y confiables que garanticen la protección de la información personal del consumidor y de la transacción misma. El proveedor será responsable por las fallas en la seguridad de las transacciones realizadas por los medios por el dispuestos, sean propios o ajenos.

Cuando el proveedor o expendedor dé a conocer su membrecía o afiliación en algún esquema relevante de autorregulación, asociación empresarial, organización para realización de disputas u otro organismo de certificación, deberá proporcionar a los consumidores un método sencillo para verificar dicha información, así como los detalles apropiados para contactar con dichos organismos, y en su caso, tener acceso a los códigos de prácticas relevantes aplicados por el organismo de certificación.

g) *Disponer en el mismo medio en que se realiza comercio electrónico, de mecanismos para que el consumidor pueda radicar sus peticiones, quejas o reclamos, de tal forma que le quede constancia de la fecha y hora de la radicación, incluyendo un mecanismo para su posterior seguimiento.*

h) *Salvo pacto en contrario, el proveedor deberá haber entregado el pedido a más tardar en el plazo de treinta (30) días calendario a partir del día siguiente a aquél en que el consumidor le haya comunicado su pedido.*

En caso de no encontrarse disponible el producto objeto del pedido, el consumidor deberá ser informado de esta falta de disponibilidad de forma inmediata.

En caso de que la entrega del pedido supere los treinta (30) días calendario o que no haya disponible el producto adquirido, el consumidor podrá resolver o termina, según el caso, el contrato unilateralmente y obtener la devolución de todas las sumas pagadas sin que haya lugar a retención o descuento alguno. La devolución deberá hacerse efectiva en un plazo máximo de treinta (30) días calendarios.

PARÁGRAFO. El proveedor deberá establecer en el medio de comercio electrónico utilizado, un enlace visible, fácilmente identificable, que le permita al consumidor ingresar a la página de la autoridad de protección al consumidor de Colombia.

Derecho de Retracto

Otro aspecto importante que trae consigo la normatividad de protección de los consumidores en el comercio electrónico, es el derecho de retracto que estos tienen al momento de adquirir bienes y servicios utilizando este mecanismo, que se encuentra fundamentado en la asimetría existente entre las partes de la negociación electrónica, quienes con posterioridad y con ocasión de la compra y recibo del producto en el lugar indicado, no se encuentran satisfechos con el producto adquirido. Por lo tanto, el empresario está obligado a informar acerca del *"derecho de retracto que le asiste al consumidor y el procedimiento para ejercerlo".* El término establecido por la ley para que el consumidor ejerza este derecho es de 5 días hábiles contados a partir de la entrega del bien o de la celebración del contrato en caso de tratarse de una prestación de servicios. Sin embargo, este derecho también genera una serie de obligaciones y deberes correlativos, por un lado, al consumidor le corresponde al momento de hacerlo efectivo realizar la devolución de los productos por los mismos medios y en las condiciones en que fueron recibidos y, por su parte, a los proveedores les corresponde realizar la devolución de la totalidad del dinero en un plazo máximo de 30 días calendario contados a partir de la fecha en la que se ejerció el derecho de retracto. Los efectos jurídicos de este derecho es la resolución del contrato y volver al estado de cosas anterior.

Es importante resaltar que, si el empresario cumple de manera adecuada el deber de información frente las condiciones objetivas y subjetivas de los productos o bienes y

servicios ofrecidos en el comercio electrónico, reduce considerablemente el riesgo de que el Consumidor ejerza el derecho de retracto, que en muchas ocasiones generan pérdidas económicas y en la credibilidad de las empresas. Probablemente si un cliente ejerce el derecho de retracto, es un cliente perdido y, la situación se hace más gravosa en el evento en que ese derecho de retracto no sea satisfecho ni cumpla con los requisitos legales establecidos, incluso podría tratarse de un doble incumplimiento que genere condiciones adversas para los empresarios.

Reversión del Pago

Al momento de la implementación del comercio electrónico y dados sus riesgos en la seguridad de la información de los clientes, una figura importante a tener en cuenta es la reversión del pago, que tiene por objeto la devolución del dinero al consumidor cuando este sea *"objeto de fraude, o corresponda a una operación no solicitada, o el producto adquirido no sea recibido, o el producto entregado no corresponda a lo solicitado o sea defectuoso"*[5]. En cuanto a los requisitos para que este derecho sea efectivo es necesario el cumplimiento de los siguientes requisitos:

a) Tratarse de venta de bienes a través de "mecanismos de comercio electrónico", internet, PSE, call center y/o cualquier otro mecanismo de televenta o tienda virtual.

[5] Artículo 51 de la ley 1480 de 2011

b) Haber realizado el pago mediante tarjeta de crédito, débito o cualquier otro instrumento de pago electrónico.

c) Que el consumidor haya presentado la solicitud dentro de los cinco (5) días hábiles siguientes a la fecha en que "*tuvo noticia de la operación fraudulenta o no solicitada o que debió haber recibido el producto o lo recibió defectuoso o sin que correspondiera a lo solicitado".* Si el producto es defectuoso o no corresponde a lo solicitado debe presentar la queja ante el empresario y devolver el producto.

d) Que el consumidor haya notificado la reclamación al emisor del instrumento de pago electrónico utilizado para realizar la compra. A ése, junto con los demás participantes del proceso de pago, le corresponde reversar la transacción al comprador.

Podríamos coincidir pues en la afirmación de que el *"nuevo estatuto del Consumidor diferencia positivamente los consumidores de los "ciberconsumidores" otorgándoles a estos últimos mecanismos propicios para contrarrestar eventuales conductas fraudulentas o engañosas en el contexto del comercio electrónico*" (Maria Lorena Florez, 2012). Lo anterior, debido a los cambios sociales que se han dado a lo largo de la historia, la globalización y la implementación de nuevas tecnologías en las actividades rutinarias de los consumidores, que han visto de cerca la evolución del comercio, que obliga a consumidores y a empresarios adaptarse con el devenir del tiempo.

Otro de los aspectos importantes en el Comercio electrónico, es el relacionado con los mecanismos de pago establecidos por los empresarios, los cuales generalmente realizan intermediaciones con diferentes proveedores de tecnologías o de las denominadas pasarelas de pago, con el ánimo de ofrecer alternativas confiables y seguras a los consumidores. Sin embargo, se debe tener en cuenta que *"los medios de pago electrónico no son inmunes a fallas de seguridad, lo cual genera para el usuario el eventual peligro de ser objeto de fraudes"* (Maria Lorena Florez, 2012), para lo cual los empresarios deben adoptar medidas de contingencias para reducir estos riesgos, de ahí que se al momento de seleccionar las pasarelas digitales y conocer a los proveedores de estos servicios se tenga una due diligence acorde con las necesidades empresariales. De igual manera, el empresario debe verificar la política de protección de Datos Personales establecidas por los proveedores de servicios de pago, ya que, según la normatividad aplicable a la materia, estos son considerados encargados del tratamiento de la información y como tal tienen unos deberes frente a los titulares y frente a sus clientes.

Por tratarse de una transacción entre desconocidos, *"se necesitan reglas relacionadas con la propiedad, a efectos de identificar los objetos del intercambio; en segundo lugar, es indispensable un sistema de pago seguro, y finamente, algún mecanismo que permita castigar las trasgresiones a dichas reglas"* (Rodríguez, 2001). De igual manera, "*en el momento de realizar un pago por medios electrónicos es de*

obligatoriedad dar información privada al comprador como dirección, nombre, apellido entre otros para así confirmar con quien se está negociando" (Álvarez, 2012)

Además de los medios de pagos ya mencionados que se encuentran en el Comercio Electrónico, está el pago a través de tarjetas de crédito o débito, mecanismo que ha tenido una gran acogida en el ámbito de consumo y que facilita de manera considerable las transacciones en línea.

Habiendo hecho un análisis acerca del comercio electrónico en Colombia, conociendo los derechos que le asisten a los consumidores electrónicos y viendo la relación y el estrecho vínculo inseparable entre la protección de los datos personales y el e-commerce, que genera seguridad y confianza en los consumidores al momento de las transacciones que realicen por este medio, daré paso al objeto de estudio de la presente investigación, relacionado con el principio de responsabilidad demostrada de la protección de los datos personales en el comercio electrónico.

13. EL PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA DE LA PROTECCIÒN DE LOS DATOS PERSONALES EN EL COMERCIO ELECTRÓNICO.

Marco introductorio

En acápites anteriores, se estudiaron los principios rectores establecidos en la ley de protección de datos personales los cuales son de vital importancia para la protección de los derechos de los consumidores, teniendo en cuenta que son

transversales en todas las operaciones adelantadas por los responsables y encargados del tratamiento de la información. También, estudiamos los principios actualizados del Comité Jurídico Interamericano sobre la privacidad y la protección de los datos personales de la OEA, en el que se encuentra entre otros el principio de responsabilidad, relacionado con el establecimiento de medidas más apropiadas para alcanzar las metas y vigilar su cumplimiento por parte de los responsables de datos personales, acordes con su estructura administrativa, tamaño empresarial y sus recursos.

Para tal fin, es importante visualizar esta relación entre la protección de los datos personales y el comercio electrónico, así como ver el crecimiento exponencial que este último ha tenido en los últimos años. También se hará un análisis de como se puede reflejar e implementar este principio de responsabilidad demostrada en toda la cadena de valor del comercio electrónico, principio que como lo veremos más adelante se encuentra establecido en el Decreto 1377 de 2013.

La protección de los datos personales en el comercio electrónico ha tenido una gran relevancia e importancia en los últimos años, debido a la gran cantidad de datos personales que son tratados a través del internet, redes sociales, plataformas digitales y en el comercio electrónico, que plantean grandes desafíos al momento de proteger los derechos de las personas como lo es el derecho a la intimidad, el buen nombre y el habeas data. Cuando vamos a adquirir productos o servicios a través de las plataformas de Comercio Electrónico dispuestas por las empresas, se

necesita realizar tratamiento de información personal de los consumidores para que pueda llevarse a cabo dicha transacción de manera satisfactoria. Es por esto que *"cuando damos nuestros datos, de manera consciente o inconsciente, confiamos en una empresa de la que no sabemos absolutamente nada más que su nombre*" (Llaneza, 2019, pág. 63), no conocemos sus Políticas de Privacidad ni sus medidas de seguridad para evitar incidentes frente a la protección de nuestra información.

De igual manera, *"la rápida adopción de las tecnologías digitales y móviles en Latinoamérica ha cambiado la manera en que los consumidores se comunican entre sí e interactúan con las marcas y productos. Y, como consecuencia de esto, ha cambiado su manera de comprar"* (BlackSip, 2017, pág. 5), esta situación explica los motivos por los cuales el Comercio Electrónico representa una oportunidad para el crecimiento de las empresas y demuestra el crecimiento exponencial que ha tenido en los últimos años y el pronóstico para los años futuros.

Máxime aún, que como lo ha manifestado la doctrina, *"vivimos en un planeta fraccionado geográficamente, pero fusionado tecnológicamente en donde la información es el principal bien que circula a través de una infraestructura global hiperconectada que sirve de soporte del ciberespacio"* (Nelson Remolina y Luisa Fernanda Àlvarez, 2018), motivo por el cual, se ha considerado que el tratamiento de los datos personales cada día es más transfronterizo y global.

Como si fuera poco, debido a la pandemia generada por la COVID-19, diferentes entidades estatales y diferentes empresas, se han visto en la necesidad de recolectar

un mayor número de datos personales para la adecuada implementación de los protocolos de bioseguridad y seguimiento de los casos positivos de este virus, para adoptar las medidas necesarias de prevención de contagios, motivo por el cual, la Superintendencia de Industria y Comercio tuvo que emitir una circular dando unas recomendaciones para el adecuado tratamiento de los datos personales recolectados para la implementación de los protocolos de bioseguridad, entre las que se encuentran, el deber de información al ciudadano sobre la norma específica que ordena la recolección de estos datos, la implementación de medidas de seguridad (técnicas, humanas y administrativas), la limitación del tratamiento de los datos únicamente para los fines indicados por el Ministerio de Salud y Protección Social y la obligación de almacenarlos durante el tiempo razonable y necesario para cumplir dichos protocolos (Superintendencia de Industria y Comercio, 2020).

También, ha aumentado el número de transacciones de las compras a través del comercio electrónico con ocasión de las restricciones en la economía adoptadas por el gobierno nacional, situación que genera que las empresas deban robustecer sus medidas de protección de datos personales y así aumentar la confianza de los consumidores y evitar vulnerar sus derechos fundamentales. Este fenómeno, fue estudiado en el informe realizado por BlackSip en el que resalta un artículo de la revista Forbes, indicando que *"las cuarentenas autoimpuestas o las determinadas por los gobiernos, debido a la latente preocupación de los*

consumidores por los lugares públicos, ofrecerán oportunidades para que el ecommerce saque todo su potencial" (BlackSip, 2020, pág. 8).

Según el informe del comportamiento del Ecommerce en Colombia durante el 2020 y perspectivas para el 2021, el Comercio electrónico ha sido uno de los sectores más relevantes durante la crisis sanitaria y economía, esto debido a que *"el cierre de los canales físicos, como una medida de contención para reducir el contagio de la pandemia del COVID-19, llevó a que tanto las empresas como los usuarios hicieran uso de los canales digitales rápidamente, trasladando sus transacciones del mundo físico al virtual"* (Cámara Colombiana de Comercio Electrónico, 2021). De igual manera, el diario La República informó que en la primera semana del confinamiento, el comercio electrónico obtuvo crecimientos superiores a 300% en América Latina, reflejando el cambio de hábito de los consumidores con ocasión de la crisis sanitaria y económica presentada (La República , 2020). Sin embargo, según el Reporte de industria denominado "El E-commerce en Colombia 2020" realizado por BlackSip en el que se estudiaron cifras presentadas por Statista, se estima que nuestro país ocupo el cuarto lugar en ventas a través del e-commerce en Latinoamérica durante el año 2019 (BlackSip, 2020), es decir, el país ya venía presentando un crecimiento exponencial anterior a la pandemia.

En dicho informe, al comparar el periodo entre enero y agosto de 2019 con el del año 2020, se evidenció un rápido crecimiento en las transacciones realizadas

mediante el Comercio Electrónico, particularmente *"en enero de 2020 el número de transacciones de compra realizadas a través de este canal creció el 52.2% respecto a enero de 2019. Por su parte, para julio de 2020, el número de transacciones, respecto a julio de 2019, creció 100,4%. Sin embargo, para agosto de 2020, el crecimiento en el número de transacciones en comparación con agosto de 2019 se redujo a 78,8%"* (Cámara Colombiana de Comercio Electrónico, 2021).

Esto quiere decir, que al comienzo de la crisis sanitaria y económica por el Covid-19 crecieron exponencialmente el número de transacciones realizadas a través del Comercio Electrónico, debido a las restricciones de movilidad y cierres de los establecimientos de comercio para evitar la propagación del virus. No obstante, lo anterior, con la reactivación económica dada a final del 2020 donde se redujeron las restricciones y se ampliaron las excepciones de movilidad y apertura de los establecimientos con las medidas de bioseguridad, se presentó una gran disminución de las transacciones mediante las plataformas virtuales, situación que se hizo más gravosa con la crisis económica acumulada y déficit de ahorro de los hogares colombianos.

Dicho crecimiento exponencial del comercio electrónico a lo largo de los últimos años, de manera correlativa, trajo consigo un crecimiento exponencial frente a las reclamaciones de los consumidores en materia de protección al consumidor. La SIC informó a través de la Delegatura de Protección al Consumidor que las quejas recibidas durante el 2020 en esta materia aumentaron en el 106% y

que las demandas presentadas ente la Delegatura de Asuntos Jurisdiccionales aumentaron en un 24,5%. De igual manera informó que se duplicaron las denuncias, pasando de 13.925 en 2019 a 28.752, argumentando que uno de los sectores donde mayor número de denuncias se registraron fue el sector del comercio electrónico (Superintendencia de Industria y Comercio, 2021).

En cuanto a las expectativas del año 2021, el informe establece que teniendo en cuenta la desaceleración económica se ha reducido el ingreso disponible de los hogares, situación que de antemano afectará el consumo. De igual manera, que las medidas de distanciamiento social se mantendrán hasta finales de 2021 o inicio de 2022, fechas en las que se tiene estimada un porcentaje de vacunación del 70% de la población para contrarrestar los efectos del COVID 19 y cuando esto ocurra volveremos progresivamente a la normalidad. Por lo tanto, se espera que para el año 2021 "*el crecimiento sea moderado, respecto a los niveles que se observaban antes de la pandemia" y "se espera que el año 2021 cierre con un crecimiento del 16% respecto del 2020"* (Cámara Colombiana de Comercio Electrónico, 2021)

Un caso emblemático de la situación antes descrita es el de Alpina, una empresa de productos lácteos, que para hacerle contrapeso a los canales de comercialización que perdieron fuerza al principio de la pandemia, se vio en la necesidad de robustecer su ecommerce. En palabras de su presidente Ernesto Fajardo en entrevista para la revista Forbes Colombia, antes de la pandemia las ventas por dicho medio no tradicional *"representaban un 2% del total, pero al cierre del año*

su participación alcanzó el 7%" (Bernal, 2021, pág. 36). Otro caso, es el de la empresa de confección de ropa infantil Offcorss, la cual según su presidenta Yaneth Londoño en entrevista para la revista Forbes Colombia, explicó que antes de la pandemia el comercio electrónico representaba el 7% de ventas de la compañía, pero que sin embargo debido a los cierres del comercio y de las tiendas físicas, se retrasaron los tiempos de entrega de sus productos en estos canales, por lo que se vieron en la necesidad de fortalecer e invertir recursos económicos y administrativos en el sistema logístico, situación que conllevó a que el e-commerce ahora represente el 17% de sus ventas totales (Bernal, 2021, pág. 28).

Una vez analizadas las cifras del Comercio electrónico en Colombia, y dado su crecimiento exponencial en lo últimos años, coincidimos con la doctrina en que es "*la vía más rápida y eficaz para la materialización de cualquier tipo de negocio a nivel mundial*" y que el mismo "*permite prescindir de una buena cantidad de formalidades o ritualidades con las que se solían acompañar la celebración de negocios tradicionales"* (Rincón, 2020, pág. 39)*;*se requiere que la legislación en esta materia se ajuste a las necesidades de estas nuevas modalidades de negociación, protegiendo los derechos de las partes al momento de las transacciones electrónicas, ya que para dicho autor uno de los obstáculos para el desarrollo del comercio electrónico es la inseguridad del uso de las TICS frente al marco jurídico existente.

Recientemente, fue publicada la investigación denominada *"Rendición de Cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital*", elaborada por Vivian Newman Pont y Maria Paula Angél Arango, en la cual, a partir de un análisis detallado de la normatividad de protección de datos personales en Colombia, se llegó a la conclusión de que no fueron considerados por el legislador los siguientes asuntos relacionados con la era digital: *i) datos sensibles inferidos, ii) datos vinculados al IP, iii) uso de cookies, iv) web crawling, v) comercialización de datos, iv) contenidos personalizados, y vii) decisiones automatizadas.* De igual manera, se discutió si los contenidos de la ley 1581 de 2012 no son suficientes para la rendición de cuentas de las EMNBD en el marco de la era digital, teniendo en cuenta el ámbito de aplicación de dicha normatividad y debido a que esta no es aplicable a las EMNBD que no tengan domicilio en Colombia, salvo que les sea aplicable la legislación colombiana en virtud de normas y tratados internacionales o el tratamiento de los datos personales en cuestión sea efectuado a través de un "Medio" situado en el territorio colombiano, motivo por el cual se consideró que todavía existe un amplio campo de mejora en el asunto en concreto.

Su importancia radica en el hecho de que el comercio electrónico abarca todas las etapas del negocio empresarial que se realice a través de esta modalidad, es decir, comprende entre otros: la oferta de productos o servicios, la publicidad dentro de la red, los mensajes de datos transmitidos, servicios pre y posventa. Es

decir, en palabras de la Cámara Colombiana de Comercio Electrónico, se trata de una noción sistémica denominada "cadena de valor"[6] que *"permite entender las relaciones entre proveedores, productores, distribuidores, comercializadores, agentes reguladores y consumidores durante los procesos de oferta y demanda de bienes y servicios comercializados en línea"* (Cámara Colombiana de Comercio Electrónico, 2018, pág. 6). Añade que dicha noción sistémica permite establecer como interactúan esos agentes, sus intercambios monetarios y los obstáculos en el desarrollo de sus vínculos comerciales. De igual manera, explica que la cadena de valor está compuesta por 5 fases interrelacionadas: a) Acceso al portal de Compra[7]; b) Compra en Línea[8]; c) Gestión de Pago[9]; d) logística de Entrega[10] y; e)

[6] La Cámara Colombiana de Comercio Electrónico establece que la cadena de valor debe percibirse como una secuencia de etapas interrelacionadas donde se desarrollan unas actividades primarias y secundarias que parten desde la apuesta a disposición del bien o servicio hasta el momento de venta de postventa del producto. (Cámara Colombiana de Comercio Electrónico, 2018)

[7] Durante esta primera fase se realiza la búsqueda de los sitios web (Marketplace o retail) a través de las cuales se accede a información sobre los productos para la compra (Cámara Colombiana de Comercio Electrónico, 2018).

[8] En esta fase el usuario decide efectuar el intercambio económico que dependiendo de su naturaleza y de los proveedores del producto puede ser de tres tipos: B2B, B2C o C2C.Aqui los pagos se pueden realizar bajo tres modalidades: pago con tarjeta, de crédito o débito, pago en punto de recaudo y pago contra entrega. (ibidem)

[9] Durante esta fase la persona puede seleccionar si el pago lo realiza con tarjeta de crédito, débito a cuenta bancaria, pago en punto de recaudo o pago contra entrega. Dependiendo de la elección puede requerir los servicios de una red procesadora de pago, pasarela de pagos o recaudador (ibidem).

[10] Una vez aprobada la compra se requieren una serie de procesos logísticos necesarios para garantizar el envío, la distribución, el seguimiento y la entrega del producto. Como fase de cadena de valor, la logística inicia desde que se recoge el paquete en el sitio designado por la tienda de comercio electrónico, se coordinan los recursos de transporte, personas y vehículos, guías de entrega y todos aquellos subprocesos que garantizan el transporte y entrega efectiva de los productos. (ibidem)

Postventa[11]. Adicionalmente, comprende una fase transversal correspondiente al uso de las TIC que soportan las actividades de la cadena de valor.

Por lo anterior, las empresas que comercialicen, ofrezcan y distribuyan sus productos o presten sus servicios a través de una red de comunicaciones como lo sería el internet, deben blindarse jurídicamente de tal manera que garanticen a cabalidad los derechos de los consumidores, transacciones que deben estar revestidas de "*seguridad, confianza y certeza, ya que en aún muchas de las empresas que practican esta actividad comercial en línea, no cuentan con la tecnología necesaria ni la adopción y aplicación de buenas prácticas comerciales que permitan generar un comercio electrónico seguro y confiable para cada uno de los intervinientes en esta nueva forma de relacionarse"* (Rincón, 2020, pág. 44).

Ahora bien, como se dijo en la parte introductoria, según la Superintendencia de Industria y Comercio, *"El Comercio Electrónico es el motor de la económica del siglo XXI y los datos personales son la moneda de la economía digital"* (Superintendencia de Industria y Comercio, 2019, pág. 1). Dicha frase, nos permite

[11] Tras haber realizado la compra, el usuario puede demandar o recibir por parte del Market place o Retail un servicio de acompañamiento para resolver dudas sobre el producto, adquirir bienes o servicios adicionales que garantizan la experiencia de uso del producto inicial. Igualmente, durante esta fase están incluidos los servicios de logística inversa del proceso, en caso de devolución o uso de servicios de garantía.

vislumbrar la importancia que tienen en el mercado actual el comercio electrónico y los datos personales, así como su vínculo estrecho e inseparable.

Es por esto, que las empresas que comercialicen sus bienes y servicios a través del comercio electrónico deben establecer unas políticas de protección de datos personales que se ajusten a su capacidad económica y a su objeto social, así como adaptar unas medidas de seguridad idóneas para proteger la información, generando seguridad y confianza a los consumidores para que realicen la negociación a través de las plataformas digitales. Para tal finalidad, dentro de la cadena de valor del comercio electrónico, los empresarios deben cumplir integralmente con los deberes que tienen como responsables de la información y velar porque las demás personas jurídicas o naturales que interactúan dentro de esa cadena como encargados del tratamiento de los datos personales también cumplan con sus deberes, con el ánimo de blindar la información de clientes, trabajadores, proveedores, contratistas y todos los intervinientes en la cadena.

Es decir, desde que los consumidores inician con la búsqueda de los bienes o servicios de su interés para la negociación electrónica (Market Place o retail), la empresa en primer lugar, debe solicitar autorización previa, expresa e informada para el adecuado tratamiento de datos personales, conservando constancia de la misma. Además, debe tener medidas de seguridad para garantizar la protección de los datos personales desde el ingreso de la plataforma, dando a conocer los términos y condiciones, así como las políticas de protección de datos personales, lo que

permitirá brindar la información necesaria para la transacción a los consumidores, generando confianza, seguridad y permitiendo la verificación de la identidad de las partes intervinientes.

Por otro lado, las empresas deben informar de manera clara y detallada al momento de la compra en línea, las características objetivas y subjetivas de los bienes y servicios objeto de la negociación, así como los términos y condiciones de esta y las políticas de protección de datos personales, con base en lo establecido en estatuto del consumidor colombiano, lo que permitirá a sus clientes tomar la decisión de adquirir los bienes o servicios ofrecidos.

De igual manera, al momento de la gestión del pago, las empresas deben como responsables del tratamiento de los datos personales, adoptar medidas de seguridad robustas que protejan la información dada por los consumidores al momento de realizar el pago a través de la plataforma electrónica, evitando la filtración de información, reduciendo el riesgo de fraude, hurto o suplantación de la identidad por parte de terceras personas inescrupulosas. Asimismo, debe garantizar que las pasarelas de pago con las que tenga convenio para el pago de sus productos, como encargados del tratamiento de la información cumplan con sus deberes y garanticen la confidencialidad y protección de los datos personales de los consumidores, así como de la información financiera utilizada para la negociación electrónica. Entre más y mejores medidas de seguridad sean adoptadas al momento de la gestión del pago por las empresas, más confianza generarán en los consumidores,

incrementando el buen nombre y “goodwill” de los establecimientos comerciales y marcas de las empresas.

También, al momento de la logística de entrega de los productos, las empresas pueden actuar como responsables del tratamiento de la información, cuando por ejemplo, solicitan y recolectan los datos necesarios de los consumidores para el envío (nombre, cédula, dirección de entrega, correo electrónico, número de contacto telefónico, entre otros), sin embargo, cuando se procede con el envío de los productos realizan convenios con empresas transportadoras que en ese orden de ideas en la cadena de valor, las que vienen siendo los encargados del tratamiento de los datos personales, motivo por el cual, se debe garantizar que tanto la empresa responsable como la transportadora encargada del tratamiento, cumplan con los deberes imperativos que se encuentran dentro de la ley de protección de datos personales.

Al momento de la postventa, se hace necesario que las empresas en primer lugar brinden a los consumidores toda la información necesaria para hacer efectivo el derecho de retracto cuando el mismo sea aplicable, también las políticas de garantías y devolución de dineros cuando haya lugar. Por otro lado, deben adoptar medidas de conservación de la información entregada por los consumidores para evitar que sea filtrada y darle un uso adecuado conforme con la finalidad del tratamiento de datos personales informada a los consumidores previa a la autorización. Adicionalmente, deben garantizar el derecho que tienen los

consumidores como titulares de la información para conocer, actualizar, suprimir y rectificar las informaciones que se hayan recolectado para la negociación electrónica y demás finalidades previstas en las políticas de protección de datos personales adoptadas.

Aunado a lo anterior, dentro de la fase transversal del uso de las TIC que realicen las empresas al momento de activación de marca, mercadeo digital, publicidad en redes sociales, radio, televisión, medios escritos, correo electrónico (Newsletter), se debe verificar que dentro de las políticas de tratamiento de datos personales, estas actividades se encuentren en las finalidades previstas, así como garantizar que en casos como publicidad a través de correo electrónico, teléfono, dirección física, entre otras, se cuente con la autorización previa, expresa e informada por parte del titular de la información, para evitar que interpongan una queja o realicen una reclamación ante la Superintendencia de Industria y Comercio, entidad que a través de la Delegatura de Protección de Datos Personales, tiene la facultad legal de imponer sanciones administrativas pecuniarias previo el agotamiento de un procedimiento administrativo sancionatorio, tal y como se ha explicado a lo largo del presente estudio. ·

Cabe resaltar que en el año 2019, la Superintendencia de Industria y Comercio a través de la Delegatura Para la Protección de los Datos Personales (en adelante la SIC) , emitió una guía en la que estudió de manera detallada e impartió una serie de recomendaciones para la protección de los datos personales en el comercio

electrónico como lo son: *(i)Cumplir las normas locales sobre el tratamiento de datos personales (TDP) cuando su proyecto de comercio electrónico tiene efectos en varios países o utiliza datos de personas ubicadas en diferentes partes del mundo"; (ii) "Implementar estrategias de responsabilidad demostrada (accountability) frente al tratamiento de datos personales (TDP) para fines de comercio electrónico"; (iii) "exigir el respeto de la política de tratamiento de datos personales a los terceros que contrata para realizar actividades de comercio electrónico"; (iv) "Efectuar estudios de impacto de privacidad"; (v) Incorporar la privacidad y la ética desde el diseño y por defecto"; (vi) "Evitar la suplantación de identidad de los consumidores; (vii) Garantizar la seguridad de la información de los consumidores"; (viii) "verificar que los datos personales fueron obtenidos lícitamente y que pueden ser usados para las actividades que comprende un proyecto de comercio electrónico"; (ix) "recolectar los datos estrictamente necesarios para fines de comercio electrónico"; (x) "dejar de contactar a las personas que no quieren recibir más publicidad y suprimir los datos de contacto cuando lo soliciten"; (xi) adoptar medidas para garantizar los principios sobre TDP en actividades de comercio electrónico"; (xii) Respetar los derechos de los titulares de los datos e implementar mecanismos efectivos para el ejercicio de los mismos"; (xiii) Utilizar herramientas de anonimización; (xiv) usar los datos de contacto en días y horas que no afecten la tranquilidad de las personas"; (xv)"incrementar la confianza y la transparencia con sus clientes y terceros titulares de datos personales*".

Lo anterior, se hizo con base en las recomendaciones sobre privacidad de la Organización para la Cooperación y el Desarrollo Económico (OCDE), en las que se señalan que las empresas deberían proteger los datos personales del consumidor, para asegurarse que su tratamiento sea legal, transparente y justo (OECD, 2016).

La Superintendencia de Industria y Comercio en dicha guía adujo que *"cualquier actividad de comercio electrónico debe ser respetuosa de, entre otros, lo que ordena el artículo 15 de la Carta Política";* motivo por el cual, presentó algunas sugerencias a quienes utilizan datos personales en desarrollo de actividades de comercio electrónico, para orientarlos y que desde su gestión se tengan en cuenta la regulación sobre el tratamiento de datos personales, evitando la vulneración de los derechos de los titulares de la información en estas actividades. En relación con el cumplimiento de las normas locales sobe el tratamiento de los datos personales, argumenta que para que el proyecto de comercio electrónico no tenga objeciones jurídicas es indispensable un estudio de los riesgos legales que se encuentran en la normatividad nacional.

Adicionalmente, que, si la empresa contrata a otra para realizar actividades de comercio electrónico, deberá exigirle a este último el cumplimiento de su Política de Tratamiento de Datos Personales. De igual forma, la SIC recomienda que las empresas fortalezcan las medidas para establecer la identidad real de las personas en la contratación, en cumplimiento del principio de veracidad que trae consigo el Tratamiento de los Datos Personales, de manera que se pueda comprobar la

veracidad de la información acerca de la identificación para evitar las suplantaciones de identidad.

Como se puede vislumbrar, en los diferentes informes y recomendaciones presentados anteriormente, se da una especial relevancia a la implementación de las estrategias de responsabilidad demostrada, a través de la cuales las empresas deben probar que han adoptado medidas apropiadas y efectivas para cumplir con las reglas sobre el tratamiento de los datos personales establecidas en la ley 1581 de 2012. Máxime aún, que la SIC[12] a través de la Delegatura de Protección de Datos Personales (Superintendencia de Industria y Comercio, 2021), informó que uno de los hallazgos más preocupantes de un estudio anual sobre las medidas de seguridad que han implementado las empresas, es que 24.424 organizaciones públicas y privadas (fueron estudiadas 33.596 organizaciones) no han puesto en marcha una política de protección para el acceso remoto a la información personal, es decir, en palabras de la SIC, no cuentan con mecanismos eficientes para proteger los datos de sus usuarios de accesos no autorizados o incidentes de seguridad. Adicionalmente, encontró que 20.594 empresas no han implementado

[12] Según la SIC: *"Las conclusiones surgen de la información suministrada por 33,596 organizaciones Responsables del Tratamiento de datos que registraron sus bases de datos en esta Entidad, desde el año 2015 hasta el 30 de septiembre de 2020. De éstas, 31.333 son empresas privadas (93.3%) y 2.263 entidades públicas (6,7%). La SIC realizó 26 preguntas sobre seguridad en el formulario electrónico del RNBD, respecto de las cuales cada organización Responsable del Tratamiento (empresa o entidad pública) solo debía manifestar SI o No".*

una política especifica que regule el acceso a la información personal de las bases de datos con información sensible, es decir, no cuentan con las medidas para proteger los datos sensibles.

En el estudio de Medidas de Seguridad en el Tratamiento de Datos Personales, realizado por la Delegatura para la Protección de Datos personales, en relación con el comparativo entre el año 2019 y el año 2020 se obtuvieron los siguientes resultados:

CONCEPTO	**AÑO 2019**	**AÑO 2020**
Número de Organizaciones evaluadas	32.763	33.596
No tienen una política de protección para acceso remoto a la información personal	88%	72,7%
No cuenta con mecanismos de monitoreo de consulta de las bases de datos	84%	69,3%
No ha implementado un procedimiento de auditoría de los sistemas de información	83%	71,3%
No tiene implementado un sistema de gestión de seguridad o un programa integral de gestión de datos	82%	67,5%

No ha implementado medidas especiales para proteger datos sensibles	79%	61,3%
No ha implementado una política de seguridad para el intercambio físico o electrónico de datos	76%	66,1%
No tiene política de auditoria de seguridad de la información	72%	63,6%
No tiene controles de seguridad de la tercerización de servicios para el tratamiento de datos	71%	61%
No implementa medidas apropiadas y efectivas de seguridad	66%	50,7%
No cuenta con herramientas de gestión de datos	63%	49,9%
No tiene políticas y procedimientos de gestión de incidentes de seguridad	62%	52,6%
Promedio de incumplimiento respecto de los ítems evaluados	**75%**	**62, 36%**

Tabla N°1. Resultados de los años 2019-2020 del Estudio de Medidas de Seguridad en el tratamiento de datos personales de la SIC. 2020

Como se puede evidenciar y con base en la información dada por la SIC, en términos generales el estudio demuestra que el cumplimiento de las medidas de seguridad en materia de protección de datos personales en comparación entre el año 2019 y 2020, mejoró en un 12,73%. Sin embargo, también muestra un gran incumplimiento de los ítems evaluados por parte de las organizaciones privadas y públicas. Al respecto, con base en información suministrada en el estudio, podemos presentar el siguiente análisis frente a los aspectos en los que se incrementó el porcentaje de cumplimiento y los aspectos de menor cumplimiento durante 2020 respecto de 2019:

Aspectos que incrementaron su porcentaje de cumplimiento de 2020 frente a 2019	**Porcentaje**	**Aspectos de menor cumplimiento de 2020 frente a 2019**	**Porcentaje**
Implementación de medidas especiales para proteger datos sensibles	**+17,7%**	No tiene política de auditoría de seguridad de la información	**+8,4%**
Creación de política de protección para acceso remoto a la información personal	**+15,3%**	No tiene políticas y procedimientos de gestión de incidentes de seguridad	**+9,4%**

Incorporación de medidas apropiadas y efectivas de seguridad	**+15,3%**	No ha implementado una política de seguridad para el intercambio físico o electrónico de datos	**+9,9%**
Uso de mecanismos de monitoreo de consulta de las bases de datos	**+14,7%**	No tiene controles de seguridad en la tercerización de servicios para el tratamiento de Datos.	**10%**

Tabla N°2. Elaboración Propia. Fuente: Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020.

Se podría concluir entonces, que en Colombia hay un elevado incumplimiento de los deberes de los responsables de la información, sean de naturaleza privada o pública, situación que pone en un alto riesgo la información de las personas, que podrían ver afectada su integridad, intimidad y buen nombre por el inadecuado tratamiento de datos personales. De ahí radica la importancia y el papel preponderante que tiene el principio de responsabilidad demostrada en el tratamiento de los datos personales.

Marco Conceptual

Una vez hecho revisado el marco introductorio y vistos los argumentos acerca de la importancia de la implementación del principio de responsabilidad demostrada por los encargados y responsables del tratamiento, pasaré a realizar el marco conceptual y jurídico de este principio en Colombia.

En materia de protección de datos personales, el artículo 4 de la ley 1581 de 2011, establece de manera específica una serie de principios que se deben adoptar al momento del tratamiento de la información, entre ellos se encuentran: a) Principio de Legalidad en materia de Tratamiento de Datos Personales[13]; b)Principio de Finalidad[14]; c) Principio de Libertad[15]; d) Principio de Veracidad o calidad[16]; e) Principio de Transparencia[17]; f) Principio de Acceso y circulación restringida[18]; g) Principio de

[13] "El Tratamiento a que se refiere la presente ley es una actividad reglada que debe ajustarse a lo establecido en ella y en las demás disposiciones que la desarrollen (ley 1581 de 2012, artículo 4).

[14] "El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al titular". (Ibidem).

[15] "El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titula. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento. (ibidem).

[16] "La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error". (ibidem).

[17] "En el tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan". (ibidem).

[18] "El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados por el Titular y/o por las personas previstas en la presente ley". (ibidem).

seguridad[19]; h)Principio de Confidencialidad[20]. Dichos principios, son valiosos para que en la práctica se respeten los derechos de los titulares de la información, de igual manera, establecen *"un límite al tratamiento indebido de los datos personales y en instrumento hermenéutico para la correcta interpretación y aplicación de las leyes sobre el tratamiento de datos personales* (Remolina, Tenorio & Quintero, 2018)

Ahora bien, el decreto 1377 de 2013 estable el Principio de Responsabilidad Demostrada. Por lo tanto, al momento de realizar el tratamiento de datos personales, las empresas en calidad de responsables o encargados del tratamiento de la información deben velar por el cumplimiento de los principios consagrados en la ley. El capítulo VI del Decreto 1377 de 2013, establece la Responsabilidad Demostrada frente al tratamiento de los Datos personales de la siguiente manera:

> *(…) "**Artículo 26**. Demostración. Los Responsables del tratamiento de Datos Personales deben ser capaces de demostrar, a petición de la Superintendencia De Industria y Comercio, que han implementado medidas apropiadas y efectivas para*

[19] "la información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento". (ibidem).

[20] "Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma" (ibidem).

cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente:

1. *La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.*
2. *La naturaleza de los datos personales objeto de tratamiento.*
3. *El tipo de tratamiento.*
4. *Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.*

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso.

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas.

Artículo 27. *Políticas internas efectivas. En cada caso, de acuerdo con las circunstancias mencionadas en lo numerales 1,2,3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar:*

1. *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 1581 de 2012 y este decreto.*
2. *La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.*
3. *La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, con respecto a cualquier aspecto del tratamiento.*

La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto". (...)

En relación con el principio de Responsabilidad Demostrada, en materia de protección de datos personales *"se refiere al modo como una organización debe cumplir en la práctica las regulaciones sobre la materia y a la manera como debe demostrar que lo hecho es útil, pertinente y eficiente"* (Nelson Remolina y Luisa Fernanda Àlvarez, 2018). Como su nombre lo indica, las empresas como responsables o encargados del tratamiento datos personales no solo deben tener responsabilidad del cumplimiento de la normatividad y sus deberes frente la protección de los datos, sino que debe acreditar mediante cualquiera de los medios probatorios establecidos en la legislación colombiana, que han adoptado las medidas apropiadas y efectivas, administrativas, técnicas y jurídicas para garantizar los derechos de los titulares de la información y minimizar los riesgos derivados de esta actividad. Dichas medidas, *"deben ser objeto de revisión y evaluación permanente para establecer su eficacia en cuanto al cumplimiento y el grado de protección de los datos personales"* (Remolina, Tenorio & Quintero, 2018, pág. 185) y esto se logra con lo que ha denominado la doctrina como el Programa integral de Gestión de Datos Personales (PIGDP), que contribuye con el buen gobierno corporativo en esta materia.

La Superintendencia de Industria y Comercio, explica que cuando hablamos de medidas apropiadas, nos referimos a "*aquellas ajustadas a las necesidades del Tratamiento de Datos" y, efectivas son las que "permiten lograr el resultado o efecto que se espera"*, concluyendo que no se deben adoptar medidas *"inoperantes, inservibles, inanes o infructuosas*" y en su lugar, se deben instaurar aquellas

"adecuadas, correctas, útiles, oportunas y eficientes con el propósito de cumplir los requerimientos legales para realizar tratamiento de datos personales" (Superintendencia de Industria y Comercio , 2019, pág. 14).

De igual manera, la Responsabilidad Demostrada ha tenido una gran importancia en el tratamiento de la información, teniendo en cuenta que con su implementación *"no sólo redundará en beneficio de la protección de los derechos de titulares de los datos personales sino que beneficiará muy positivamente a las organizaciones porque les permitirá maximizar el uso inteligente de la información, aumentar su nivel de competitividad y consolidar su buena reputación empresarial o institucional*" (Nelson Remolina y Luisa Fernanda Àlvarez, 2018).

Este principio que tiene más de 30 años, también es conocido con el término de "accountability" e inicialmente se enfocaba únicamente en la responsabilidad, sin embargo, con su implementación en diferentes marcos normativos, se incluyó la obligación de los responsables y encargados del tratamiento de la información de demostrar el cumplimiento de las normas sobre la protección de Datos Personales, motivo por el cual, *"deben ser responsables del cumplimiento efectivo de las medidas que implementen los principio de privacidad y protección de Datos*" (Superintendencia de Industria y Comercio, 2016).

En este sentido, el principio de responsabilidad demostrada se encuentra orientado a que las empresas efectivamente implementen medidas hechas a su medida que garanticen el adecuado tratamiento de los datos personales, es decir, se deben diseñar

e implementar con base en su capacidad económica, financiera, administrativa y adicionalmente teniendo en cuenta la naturaleza de los datos recolectados, la cantidad, la finalidad del tratamiento, entre otras cuestiones, máxime aún si se tratan datos de naturaleza sensible, entendidos estos como aquellos que *"afectan la intimidad del Titular o cuyo uso indebido pueden 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 posición así como los datos relativos a la salud, a la vida sexual y los datos biométricos* (Congreso de la República de Colombia, 2012).

Lo anterior, significa que los responsables no solo deben diseñar en el papel unas políticas de privacidad, deben implementarlas y velar por su cumplimiento, sino que además tienen que demostrar de manera efectiva que realmente se están llevando a cabo en su organización. En palabras de la Superintendencia de Industria y Comercio, "*El reto de las Organizaciones frente al Principio de Responsabilidad Demostrada va mucho más allá de la mera expedición de documentos o redacción de Políticas. Se trata de una actividad constante que exige demostrar un cumplimiento real y efectivo en la práctica de sus labores*" (Superintendencia de Industria y Comercio , 2019). En otra de sus guías, la SIC es enfática en que afirmar que dichas:

"Políticas internas efectivas no pueden limitarse a reproducir los textos legales ni son meras declaraciones de principios. Por el contrario, la adopción de políticas internas efectivas parte del desarrollo de un Programa Integral de Gestión de Datos Personales, que debe ser el resultado de un proceso de debida diligencia al interior de la organización que permita formularlo" (Superintendencia de Industria y Comercio, 2016, pág. 7)

Para tal fin, recomienda entrenar periódicamente a los trabajadores y contratistas de las organizaciones para el adecuado tratamiento de los datos personales dentro de su organización, para lo que se requiere de un mayor compromiso por parte de las empresas para cumplir cabalmente sus deberes y las normas en materia de protección de datos personales.

Ahora bien, el Principio de Responsabilidad Demostrada también debe ser aplicado en debida forma por las empresas al momento de la comercialización de sus bienes y servicios a través del comercio electrónico. En la medida en que se adopten medidas técnicas y efectivas para la protección de los datos personales en las transacciones electrónicas, mayor será la seguridad del tratamiento y la confianza de los Consumidores como titulares de la información incrementará. Al respecto, la Superintendencia de Industria y Comercio, al citar a Ernesto Barrera Duque, resalta que la confianza se entiende como:

"la expectativa de que se puede contar con la palabra del otro y de que se emprenderán acciones positivas y beneficiosas entre las partes de manera

recíproca. Cuando existe la confianza, la persona cree que la empresa es fiable, cumple su palabra, es sincera, integra y lleva a cabo las acciones prometidas" (Superintendencia de Industria y Comercio , 2019, pág. 19).

Por lo anterior, se entiende que la confianza es un elemento fundamental para el crecimiento de las empresas que realicen un adecuado tratamiento de los datos personales de los consumidores que adquieren los bienes y servicios a través del comercio electrónico.

La Guía para la Implementación del Principio de Responsabilidad Demostrada en las transferencias internacionales de datos personales, emitida por la Superintendencia de Industria y Comercio, trae consigo las siguientes recomendaciones para la generación de confianza en los clientes y los titulares de los datos personales: *"a) Mantener canales abiertos de comunicación y divulgación de los datos personales...; b) Implementar un sistema efectivo de debida y oportuna atención de quejas y reclamos; c) Cumplir en la práctica lo que se dice o promete en las políticas de tratamiento de la información".* (Superintendencia de Industria y Comercio , 2019)

En cuanto a los beneficios de la implementación de la Responsabilidad Demostrada Frente al Tratamiento de los Datos Personales, se puede traducir en una mayor protección, confianza y seguridad de la empresa a favor de los Titulares, lo que conlleva necesariamente a un incremento de la comercialización de sus productos a través del Comercio Electrónico. Si un consumidor percibe que la empresa tiene medidas de seguridad idóneas, que cumple con la protección de los derechos de los consumidores

y da un adecuado tratamiento a los datos personales, lo más probable es que ese cliente vuelva a adquirir bienes y servicios con dicha empresa. De igual forma, los beneficios que trae consigo la Responsabilidad Demostrada es la reducción de los riesgos que pueden ser objeto de una sanción administrativa pecuniaria por parte de la Superintendencia de Industria y Comercio en cabeza de la Delegatura de Protección de Datos Personales.

Se puede concluir diciendo que este principio demanda menos retórica y más acción en el cumplimiento de los deberes impuestos por las normas de tratamiento de datos personales, y su éxito depende del compromiso real de todos los miembros de una organización, en especial de sus directivos. El reto va mucho más allá de la expedición de documentos porque se requiere que en la práctica las organizaciones demuestren el cumplimiento real y efectivo cuando realicen sus funciones, garantizando los mandatos constitucionales y legales sobre la protección de datos personales en beneficio de los titulares de la información (Remolina, Tenorio & Quintero, 2018).

14. RECOMENDACIONES PARA LA IMPLEMENTACIÓN DE UN PROGRAMA DE GESTIÓN DE DATOS PERSONALES EN EL COMERCIO ELECTRONICO CON BASE EN LA GUIA DE IMPLEMENTACION DEMOSTRADA DE LA SIC.

Una de las maneras que tienen los encargados y responsables del Tratamiento de la información para cumplir a cabalidad con el Principio de responsabilidad demostrada en el tema objeto de estudio, es la de implementar dentro de sus organizaciones un Programa de Gestión de Datos Personales en el Comercio Electrónico, para lo cual se recomendaciones para su implementación, con base en la Guía Para la Implementación del Principio de Responsabilidad Demostrada (Accountability) elaborada por la Superintendencia de Industria y Comercio, como entidad de Protección de Datos Personales en Colombia.

Para este fin, la Guía desarrolla los siguientes elementos esenciales para la implementación de dicho programa: 1. Compromiso de la Organización y 2. Controles del Programa. Cabe resaltar, que la guía explica estos elementos de manera general, dando unas adecuadas recomendaciones para el tratamiento de los datos personales, sin embargo, con el ánimo de tratar el tema objeto de estudio, se adecuarán los elementos para un adecuado programa de gestión de los datos en el comercio electrónico.

14.1 COMPROMISO DE LA ORGANIZACIÓN.

Como se ha mencionado anteriormente, dos de los baluartes importantes en el comercio electrónico, son la seguridad y confianza que las empresas generen en los consumidores al momento de realizar las transacciones electrónicas. Esto se traduce en la necesidad que tienen las empresas para adoptar medidas eficaces para garantizar la seguridad de la información de los consumidores. Para ello, se requiere de un total compromiso de las organizaciones, en especial, de sus directivos y alta gerencia,

teniendo en cuenta su capacidad económica y su tamaño empresarial. Según las recomendaciones dadas por la SIC (Superintendencia de Industria y Comercio, 2016), para lograr estos objetivos se debe contar con el apoyo *a) desde la alta dirección, b) Oficial de Protección de Datos y; c) Presentación de Informes.*

a) Desde la Alta Gerencia: el apoyo de la alta gerencia es elemental para la adecuada implementación del Programa Integral de Gestión de Datos Personales, con el ánimo de que se implemente en todas sus áreas de manera exitosa. Para este propósito, la SIC en la precitada guía de implementación, resalta que la alta dirección debe *(a) "designar a la persona idónea o al área que asumirá la función de protección de Datos Personales; (b) aprobar y monitorear el Programa Integral de Gestión de Datos Personales, y (c) informar que manera periódica los órganos directivos sobre su ejecución".* Seguro que, si se siguen estas recomendaciones por parte de las directivas de una organización, generará confianza y seguridad en sus clientes y consumidores, lo que generará un mayor incremento en sus ganancias y buena imagen de la compañía frente a los clientes, socios, proveedores, entidades bancarias, entre otros

b) Designar a la persona idónea o el área que asumirá la función de protección de Datos personales: más que una recomendación, es una de las obligaciones de los encargados y los responsables del tratamiento de los datos personales, establecidas el artículo 23 del decreto 1377 de 2013. Esta área o la

persona designada, se encargará de garantizar que se cumpla a cabalidad el Programa de Gestión de los Datos Personales, es decir, velará por que la organización o empresa, cumpla con sus deberes como responsables o encargados del tratamiento de la información. Por lo tanto, debe ser una persona que conozca de manera detallada las políticas de privacidad implementadas, que conozca de manera detallada toda la organización de la empresa, la logística para la comercialización de los bienes o la prestación de los servicios a través de la plataforma e-commerce, conozca la información que se recolecta, las finalidades de los datos personales recolectados (en especial los datos sensibles, los relacionados con la información de pago y entrega), las bases de datos existentes en la compañía, los derechos que tienen los titulares de la información, así como los mecanismos de atención a quejas y reclamos, para darle el trámite respectivo. Además, debe ser una persona que tenga conocimiento sobre la normativa en materia de protección de Datos Personales. Cabe resaltar, que la SIC (Superintendencia de Industria y Comercio, 2016) citando un estudio denominado "*A privacy office guide to demostrating accountability*" de NYMITY, estableció un manual de funciones que debe cumplir el oficial de Protección de Datos dentro de las organizaciones[21].

[21] Dentro de las actividades que deben desarrollar los Oficiales de Protección de Datos se encuentran las siguientes: *a) "Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales; b) coordinar la definición e implementación de los*

c) Presentación de Informes: esta recomendación implica que las empresas tengan implementados sistemas para informar y comunicar de manera interna el seguimiento y la ejecución del Programa de Gestión de los Datos Personales y las políticas de privacidad que se tengan implementadas. De igual manera, para dar a conocer los procedimientos de atención de quejas y reclamos frente al tratamiento de los datos personales por parte de los titulares de la información y lo que deben hacer en caso de que se presente una vulneración de la seguridad o de los demás derechos de los titulares. Estos informes deberán ser presentados a la alta gerencia, a los socios y accionistas para que se encuentren plenamente informados del cumplimiento de la normatividad en materia de protección de

---

controles del programa integral de gestión de datos personales; c) servir de enlace y coordinador con las demás áreas de la organización para asegurar la implementación transversal del Programa Integral de Gestión de Datos Personales; d) impulsar una cultura de protección de datos dentro de la Organización; e) mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo; f)registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC; g)obtener las declaraciones de conformidad dela SIC cuando sea requerido; h) revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia; i) analizar las responsabilidades de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos personales para todos los empleados de la compañía; j) realizar un entrenamiento general en protección de datos personales para todos los empleados de la compañía, k) realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización; l) integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización, m) medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos, n) requerir que dentro de los análisis de desempeño de los empleados se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales; o) velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal, o) acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio; p)Realizar seguimiento al Programa Integral de Gestión de Datos Personales".

datos personales, ya que minimiza los riesgos de sanciones administrativas pecuniarias y garantiza seguridad y confianza frente a sus clientes y proveedores.

14.2 CONTROLES DEL PROGRAMA.

Otras de las recomendaciones dadas por la Superintendencia de Industria y Comercio, para la adecuada implementación de un Programa de Gestión de Datos Personales, es la del desarrollo y puesta en marcha de controles que le permitirán al oficial de protección de datos desarrollar dicho programa, para asegurar que las políticas se implementen dentro de las organizaciones (Superintendencia de Industria y Comercio, 2016). Según la SIC, dentro de esos controles se encuentran los siguientes:

a) **Procedimientos Operacionales:** tal y como lo establece la SIC este control busca que las empresas implementen procedimientos administrativos con base en las políticas de protección de datos personales, para el adecuado manejo de los riesgos inherentes al tratamiento de la información. En cuanto a este control en la protección de los datos personales a través del comercio electrónico, se requiere que las empresas adecuen sus políticas de privacidad teniendo en cuenta la información que se recolecta para las transacciones electrónicas, así como las finalidades especificas autorizadas por los titulares de la información, para evitar los riesgos derivados de la vulneración de sus derechos.

b) **Inventario de las Bases de Datos con Información Personal:** la SIC recomienda que los responsables del tratamiento de la información deben conocer que datos personales almacenan y como los utilizan teniendo en cuenta las finalidades de su tratamiento. Es por esto, que las empresas deberán tener claridad de que bases de datos tienen como seria las bases de datos con información de clientes, proveedores, aliados comerciales, trabajadores, contratistas, socios, personas inscritas en el Newsletter, peticionarios, entre otros, que permitan conocer la naturaleza de los datos recolectados como lo seria datos públicos, privados, semiprivados y sensibles, para adoptar las medidas de seguridad necesarias para su protección. Además, es una obligación de algunos de los responsables, registrar dichas bases en el Registro Nacional de Bases de Datos.

c) Los responsables del tratamiento de la información no solo deben redactar e implementar unas políticas de protección de datos personales que deben incluir los ítems que la normativa en esta materia imponen, sino que además deben dar a conocer estas políticas a sus empleados, en especial, de aquellos que manejen y realicen un tratamiento de la información recolectada por la empresa, para evitar el riesgo de vulneración de los derechos de los titulares y sanciones administrativas por parte de la entidad de protección de datos personales. Es importante que esas políticas se cumplan a cabalidad por todos los empleados y en toda la cadena de producción, así como en las

transacciones electrónicas para garantizar el efectivo cumplimiento de los deberes de los responsables y los derechos de los titulares de la información.

d) **Sistemas de administración de riesgos asociados al tratamiento de datos personales.** Según la SIC (Superintendencia de Industria y Comercio, 2016) las organizaciones deben identificar y manejar los riesgos asociados al tratamiento de los datos personales. Para tal fin, se tiene que desarrollar un sistema de administración de riesgos que debe ser acorde con la estructura organizacional y procedimientos internos asociados al tratamiento de los datos personales, la cantidad de base de datos y tipos de datos tratados. Es por esto, que recomienda que el sistema de administración de riesgos debe tener en cuenta las siguientes etapas:

    - Identificación de los riesgos a que se ven expuestos los datos personales en su tratamiento.
    - Medición de la posibilidad de materialización de los riesgos relacionados con el tratamiento de la información.
    - Control para mitigar los riesgos a los que se ven expuestos los datos personales, para reducir la posibilidad de materialización de los mismos.
    - Monitoreo y seguimiento constante para velar porque las medidas establecidas sean las adecuadas.

Este sistema de administración de riesgos asociados al tratamiento de los datos personales es importante para la adecuada implementación del Programa y permite que las empresas reduzcan la materialización de los riegos y las posibles sanciones administrativas por parte de la Superintendencia de Industria y Comercio como entidad de protección de datos personales. Máxime aun, cuando las empresas realizan la comercialización de sus bienes y servicios a través del comercio electrónico, ya que puede verse involucrada información de naturaleza sensible y se necesitan adoptar mecanismos de seguridad que permitan su adecuado tratamiento y generen confianza entre los consumidores.

e) Requisitos de formación y Educación

Una de las recomendaciones dadas por la SIC, es la de formar y educar a todos los empleados de la información con el ánimo de que conozcan el Programa Integral de Gestión de Datos Personales. De nada sirve tener unas políticas de tratamiento de Datos Personales si no son difundidas, conocidas ni mucho menos aplicadas por los empleados, ya que los datos personales son tratados día a día por ellos en el ejercicio de sus funciones. Es importante, que conozcan las bases de datos que tiene la empresa, la naturaleza de los datos, las finalidades del tratamiento, los derechos de los titulares y los deberes de los responsables, pero, además, que conozcan de manera detallada los mecanismos internos de respuestas a quejas y reclamos por parte de los titulares. De igual manera, es necesario que conozcan las sanciones administrativas a las que se ve

expuesta la empresa, desde multas, hasta la prohibición del tratamiento de datos personales que podrían llevar incluso al cierre de la compañía.

Si bien, el decreto 1377 de 2013 establece en su artículo 17 que para la "*difusión del aviso de privacidad y de la política de tratamiento de la información, el responsable podrá valerse de documentos, formatos electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular*", lo cierto es que dichas políticas deben ser difundidas también internamente para su cabal cumplimiento por parte de los empleados y contratistas, quienes en todo caso podrán respectivamente ser considerados como titulares o encargados de la información dentro de la misma organización, motivo por el cual, se recomienda que en sus contratos se incluyan cláusulas de protección de datos personales, en la que se reconozca tanto los derechos que tienen como los deberes frente al tratamiento de la información en el ejercicio de sus funciones.

f) Protocolos de Respuesta en el Manejo de Violaciones e incidentes.

La SIC resalta que para la adecuada implementación del Programa Integral de Datos Personales *"debe involucrar un componente de gestión de riesgos, internos y externos, que le permita identificar sus vulnerabilidades a tiempo y enfocar sus recursos a la adopción de medidas de mitigación de riesgo que minimicen dicho impacto tanto para la organización como para los titulares de la información"* (Superintendencia de Industria y Comercio, 2016). Es por esto,

que se requiere de un procedimiento interno, así como un área encargada para el manejo de los incidentes o vulneraciones a la privacidad de los archivos digitales o físicos en los que se recolectan los datos personales de los titulares de la información.

Este es quizás uno de los puntos más importantes que debe tener el Programa de Gestión de Datos Personales de una empresa y con mayor razón si la empresa comercializa sus bienes o servicios a través del comercio electrónico, ya que como hemos visto es una herramienta que permite por un lado llegar a un mayor número de consumidores y permite reducir las transacciones, generando una relación de beneficios mutuos tanto para la empresa como para sus clientes. Sin embargo, la empresa debe adoptar mecanismos idóneos de seguridad para garantizar el adecuado tratamiento de los datos personales para generar confianza en sus consumidores y evitar todos los riesgos inherentes al tratamiento de datos personales como lo puede ser la suplantación de identidad, el cual ha sido denunciado en múltiples ocasiones ante la Superintendencia de Industria y Comercio, quien informó que en lo que va del año 2021 se han presentado 695 quejas por suplantación de identidad y en el año 2020 se presentaron 1599 (Superintendencia de Industria y Comercio, 2021).

De igual manera, se debe tener en cuenta que en el evento en que ocurra una violación o incidente en la seguridad de los datos personales que ponga en

riesgo el tratamiento o los derechos de los titulares de la información, sea cual sea su naturaleza, es una obligación de la empresa reportar el incidente ante la Superintendencia de Industria y Comercio como entidad encargada de la Protección de los Datos Personales. Al respecto, el literal "n" del artículo 17 de la ley 1581 de 2012, establece que es una obligación de los responsables del tratamiento de los datos personales la de *"informar 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".*

También, el informar de manera clara y oportuna a la autoridad de protección de datos personales sobre las violaciones a los códigos de la seguridad que haya puesto en riesgo o vulnerado los derechos de los titulares, puede constituirse como un criterio de atenuación frente a una posible sanción administrativa pecuniaria. Así ha sido señalado en el literal f del artículo 24 de la ley 1581 de 2012, en el que se establece que será criterio para graduar las sanciones el *"reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar"*.

Asimismo, las empresas deben tener implementado dentro de sus Políticas, mecanismos de atención a las quejas y reclamos por parte de los titulares de la información, que deben adaptarse a las necesidades de la empresa y a sus recursos económicos y deben estar basados en los términos señalados en la ley

para tal fin. Por ejemplo, el decreto 1377 de 2013 en su artículo 23 señala que "*todo responsable y encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los titulares para el ejercicio de los derechos a que se refiere la ley 1581 de 2012 y el presente decreto".* Por su parte, la ley 1581 de 2012, trae consigo en sus artículos 14 y 15 los procedimientos para atender las consultas y los reclamos, estableciendo los términos máximos que deben ser tenidos en cuenta para su atención oportuna y los casos en los que es procedente.

g) Gestión de los encargados del tratamiento en las transmisiones internacionales de datos personales.

En primer lugar, las transmisiones internacionales se refieren *"a la entrega o envío de datos personales por un responsable al encargado del tratamiento de ellos"* (Superintendencia de Industria y Comercio, 2021)**,** caso en el cual, tanto el responsable como el encargado de la información deben cumplir a cabalidad con sus deberes establecidos en los artículos 17 y 18 respectivamente de la ley 1581 de 2012. De igual manera, el decreto 1377 de 2013 en su artículo 24 numeral 2 resalta que estas transmisiones no *"requerirán ser informadas al titular ni contar con su consentimiento cuando exista un contrato en los términos del artículo 25 siguiente"*.

Es por esto que la SIC (Superintendencia de Industria y Comercio, 2016) considera que este punto es otro de los requisitos indispensables para una

adecuada implementación del Programa Integral de Gestión de Datos Personales en las empresas, motivo por el cual recomienda que en las empresas deben tener mecanismos para que el encargado reporte al Responsable los incidentes de seguridad de la Información; realización de auditorías externas y/o internas, acuerdos entre los encargados y sus empleados para el cumplimiento de las políticas de protección de datos personales y los deberes inherentes a su posición, entre otras medidas, para evitar incidentes de seguridad y la vulneración de los derechos de los titulares.

En el comercio electrónico, es frecuente que las empresas pongan a disposición de los consumidores pasarelas de pagos que permitan realizar las transferencias electrónicas de manera confiable y segura, en este caso, las pasarelas son consideradas como encargados del tratamiento de la información. Lo mismo sucede, cuando las empresas contratan servicios de otras compañías para el diseño y administración de la página web donde se encuentra alojado el sistema E-commerce; también contratan con empresas de transporte para el envío de sus productos a los consumidores finales, empresas que son consideradas en todo caso como encargados del tratamiento y por ende deben cumplir con las políticas de protección de los responsables, las suyas y los deberes establecidos en la ley.

De ahí, radica la necesidad de estudiar de manera detallada a los proveedores, para garantizar que también tengan unas políticas de privacidad

adecuadas y medidas de seguridad robustas que permitan generar confianza tanto a la empresa contratante como a los consumidores, reduciendo al máximo los riesgos de incidentes de seguridad frente al tratamiento de la información.

h) Comunicación Externa.

Según la Superintendencia de Industria y Comercio los responsables deben desarrollar un procedimiento para dar a conocer a los titulares sus derechos de acceder a sus datos personales, actualizarlos, corregirlos, eliminarlos y revocar la autorización otorgada, todo esto con base en lo establecido en la normatividad en materia de protección de datos personales en Colombia.

Este deber de información es importante, para que las personas al momento de otorgar la autorización del tratamiento a los responsables tomen esta decisión de manera libre y espontánea, conociendo el uso que se le dará a sus datos personales y la finalidad de su tratamiento, así como sus derechos y los mecanismos de atención a las quejas y reclamos.

Esto genera confianza entre las empresas y los consumidores, sin perjuicio del contenido del deber de información que trae consigo el estatuto del consumidor para que los clientes al momento de tomar la decisión de realizar una transacción electrónica lo hagan conociendo los beneficio y los riesgos que trae consigo el tratamiento de los datos personales en el comercio electrónico.

Por último, la Superintendencia de Industria y Comercio (Superintendencia de Industria y Comercio, 2016) es enfática al resaltar que es muy importante desarrollar un Programa Integral de Gestión de Datos Personales en las empresas, pero también considera que es importante mantener ese programa para garantizar su eficacia permanente, el cumplimiento y la adherencia a estándares de Responsabilidad Demostrada, lo que implica el supervisar, evaluar y revisar periódicamente el programa para garantizar su efectividad y demostrar la debida diligencia en el tratamiento de los datos personales por parte de los Responsables de este.

Sin duda alguna, si se llevan a cabo las recomendaciones planteadas en el presente acápite, los encargados y responsables del tratamiento de la información cumplirán no solo con los principios rectores de la protección de los datos personales establecidos en la ley 1581 de 2021, sino que además estarán cumpliendo con el principio de responsabilidad demostrada del tratamiento de la información durante toda la cadena de valor que trae consigo el comercio electrónico. Esto, conllevaría a que se redujeran considerablemente las sanciones administrativas impuestas por la Superintendencia de Industria y comercio y se protegerían cabalmente los derechos fundamentales de los titulares de la Información, teniendo en cuenta que las recomendaciones contribuyen a que los encargados y responsables, adopten medidas

administrativas adecuadas que garanticen la seguridad de la información y genere confianza entre los consumidores.

15. CONCLUSIONES

- La protección de los datos personales es importante al momento de la implementación del comercio electrónico en las empresas, genera seguridad y confianza en los consumidores al momento de las transacciones electrónicas.
- Si bien en Colombia hay una normatividad que regula la protección de los datos personales, muchas empresas no conocen de manera detallada cuáles son sus deberes como responsables del tratamiento de la información, situación que pone en riesgo la privacidad y los derechos de los titulares, generando un alto riesgo de una sanción administrativa por parte de la Autoridad de Protección de Datos Personales en Colombia.
- Una adecuada implementación de un Programa Integral de Gestión de Datos personales requiere que sea conocido de manera detallada por todos los empleados y contratistas del Responsable y/o Encargado del Tratamiento de la Información.
- El Programa Integral de Gestión de Datos Personales, requiere una inversión de recursos económicos, técnicos y administrativos por

parte de las empresas y de un real compromiso por parte de la Alta Dirigencia para su implementación y Seguimiento.

- Este programa permite acreditar que las empresas han cumplido a cabalidad con el principio de responsabilidad demostrada en el tratamiento de los datos personales, en especial cuando este se realiza con información de clientes que realizan las transacciones a través del comercio electrónico, logrando comprobar una debida diligencia por parte de los responsables.
- Los consumidores también tienen el deber de conocer de manera detallada no solo acerca de la información de los productos que van a adquirir, sino de las finalidades del tratamiento de los datos personales requeridos para la transacción electrónica, esto les permitirá tener conciencia acerca del uso de su información para tomar la decisión de otorgar la autorización de manera previa, expresa e informada.
- Las empresas deben adaptar un Programa Integral de Gestión de Datos Personales, que les permita garantizar el cumplimiento de los derechos de los titulares, el cumplimiento de sus deberes y la reducción de los riesgos de las sanciones tanto pecuniarias como administrativas que puede imponer la autoridad de protección de datos personales en ejercicio de sus facultades legales.

- Las empresas deben comprender que tanto los datos personales como la implementación de un sistema de comercio electrónico, es necesario para llegar a un mayor número de consumidores, lo que implica un incremento de sus ingresos y un mayor reconocimiento de la marca y reconocimiento empresarial.

16. BIBLIOGRAFÍA

16.1 LIBROS

Alexy, R. (2007). Teoría de la argumentación Jurídica. La teoría del discurso racional como teoría de la fundamentación jurídica. Madrid: Centro de Estudios Políticos y Constitucionales.

Camargo, P. P. (2013). El Hábeas Data- Derecho a la Intimidad. Bogotá, D.C.: Leyer Editores.

Cárdenas, M. (2021). Cómo Avanza Colombia (Primera ed.). Bogotá: Penguin Random House Grupo Editorial SAS. Recuperado el 17 de 10 de 2021.

Dworkin. (2010). Los derechos en serio. Barcelona: Ariel.

Friedman, T. (2005). La tierra es plana

Gaiero , B., & Soba , I. (2010). *La Regulación Procesal del Habeas Data.* Buenos Aires: Editorial B de F.

Jiménez, F. (2018). *Protección Jurídica del Conocimiento y la tecnología en la empresa.* Bogotá: Editorial Temis SA.

Llaneza, P. (2019). Datanomics. Barcelona: Editorial Planeta S.A.

López, E. C. (2016). Derecho Mercantil Consuetudinario: el poder de las prácticas de los agentes económicos. Legis.

Martínez, J. G. (2017). *Ley de Habeas Data en las Instituciones Educativas.* Bogotá: Editorial Magisterio.

Newman, V. (2015). *Datos Personales en información Pública.* Bogotá D.C.: Centro de Estudios de derecho, Justicia y Sociedad, Dejusticia.

Rawls, J. (1997). *Teoría de la Justicia.* Fondo de la Cultura Económica.

Remolina, N. (2006). *Aspectos Legales del Comercio Electrónico, la contratación y la empresa electrónica.* Bogotá D.C.: Universidad de los Andes.

Remolina, Tenorio & Quintero. (2018). *De la responsabilidad demostrada en las funciones misionales de la Registraduría Nacional del Estado Civil.* Bogotá: Temis S.A. Recuperado el 08 de junio de 2021

Rincón, E. (2020). *Derecho del Comercio Electrónico y del Internet.*

Rodríguez, G. (2001). El Comercio Electrónico. Algunas Nociones de Seguridad

Suárez, J. J. (2016). El fundamento de los Principios Jurídicos: una cuestión problemática. *Civilizar 16*, 51-62.

16.2 ARTÍCULOS

16.2.1 ARTÍCULOS DE INTERNET

Nelson Remolina y Luisa Fernanda Àlvarez. (Junio de 2018). Guia GECTI para la implementaciòn del principio de responsabilidad demostrada-accountability- en las transferencias internacionales de datos personales: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Guia-GECTI-accountability-2018-Remolina.pdf

Cámara Colombiana de Comercio Electrónico. (2018). Marco de Estadísticas del Comercio Electrónico en Colombia. Bogotá D.C: https://docplayer.es/117019468-Marco-de-estadisticas-del-comercio-electronico-en-colombia.html

Cámara Colombiana de Comercio Electrónico. (2021). Informe Comportamiento del e-commerce en Colombia durante 2020 y perspectivas 2021. Bogotá D.C.: https://www.ccce.org.co/wp-content/uploads/2020/10/informe-comportamiento-y-perspectiva-ecommerce-2020-2021.pdf

Comité Jurídico Interamericano CJI de la Organización de los Estados Americanos. (2021). Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con Anotaciones.: http://www.oas.org/es/sla/cji/docs/CJI-doc_638-21.pdf

Fundación para la Libertad de Prensa-FLIP. (2020). *Violaciones a la Libertad de Prensa.* Bogotá D.C.

OECD. (2016). *Recommendation of the council on consumer protection in E-commerce: https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf*

Superintendencia de Industria y Comercio. (2019). *Guía para la implementación del principio de Responsabilidad Demostrada en las transferencias internacionales de datos personales.* Bogotá D.C.: https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales(1).pdf

Superintendencia de Industria y Comercio. (2016). *Guía pata la implementación del Principio de Responsabilidad Demostrada (Accountability).* Bogotá D.C: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Superintendencia de Industria y Comercio. (2019). *Guía sobre el tratamiento de datos personales para fines de comercio electrónico.* Guía, Bogotá D.C. Recuperado el 22 de septiembre de 2020: https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico(1).pdf

Superintendencia de Industria y Comercio. (22 de mayo de 2019). *SIC.* Obtenido de https://www.sic.gov.co/Rappi-y-Banco-Falabella-sancionados-por-incumplir-Ley-de-Proteccion-de-Datos

Superintendencia de Industria y Comercio. (2020). *Circular Externa N°008 de 2020.* Bogotá D.C..: https://www.sic.gov.co/sites/default/files/normatividad/082020/CIRCULAR%20DATOS%2018%20DE%20AGOSTO.pdf

Superintendencia de Industria y Comercio. (2021). *Guía para la implementación del Principio de Responsabilidad Demostrada en las transferencias internacionales de Datos Personales.* Bogotá D.C.: https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADas%20para%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf

Superintendencia de Industria y Comercio. (2021). *Informe de Rendición de Cuentas septiembre de 2020 a agosto de 2021*. Bogotá. Recuperado el 16 de octubre de 2021.: https://www.sic.gov.co/sites/default/files/files/2021/SIC_Informe%20de%20Rendici%C3%B3n%20de%20Cuentas_Sep%202020%20a%20Agos%202021.pdf

Superintendencia de Industria y Comercio. (11 de marzo de 2021). *Más de 24 mil empresas no tienen mecanismos eficientes para proteger los datos de sus usuarios de accesos no autorizados.* Obtenido de: https://www.sic.gov.co/slider/m%C3%A1s-de-24-mil-empresas-no-tienen-mecanismos-eficientes-para-proteger-los-datos-de-sus-usuarios-de-accesos-no-autorizados

Superintendencia de Industria y Comercio. (13 de junio de 2021). *Número de quejas recibidas en la Superindustria por suplantación de identidad entre 2018 y 2021*. Recuperado el 18 de junio de 2021, de https://www.linkedin.com/posts/superintendencia-de-industria-y-comercio_cuidatusdatos-activity-6809891156218957824-0OpE

Superintendencia de Industria y Comercio. (17 de marzo de 2021). *Superintendencia alerta sobre aumento de las denuncias de los consumidores.* Obtenido de https://www.sic.gov.co/slider/superindustria-alerta-sobre-aumento-de-denuncias-de-los-consumidores

16.2.2 ARTICULOS DE REVISTA

Bernal, C. (Junio-Julio de 2021). ¿Por qué Offcorss le agradece al 2020? *Forbes Colombia* (16), 28. Recuperado el 17 de octubre de 2021.

Bernal, C. (Julio-Agosto de 2021). El Efecto Alpina. *Forbes Colombia* (16), 36. Recuperado el 2021 de octubre de 17.

María Lorena Flórez, N. R. (07 de junio de 2012). La Protección del Consumidor en el contexto del comercio electrónico. *Revista de Derecho, comunicaciones y Nuevas Tecnologías*, 9. Recuperado el 23 de enero de 2021

Álvarez, J. F. (2012). Problemas de la regulación actual en materia de comercio electrónico, armonización y Firmas Digitales. (EAFIT, Ed.) *Journal of International Law*, *3*(02).

BlackSip. (2017). *6 estrategias digitales para tu ecommerce de consumo masivo.* Bogotá D.C. Recuperado el 23 de abril de 2021

BlackSip. (2020). *El e-Commerce y el entorno digital en tiempos de cuarentena.* Bogotá D.C. Recuperado el 23 de abril de 2021

BlackSip. (2020). *Reporte de Industria: El E-commerce en Colombia 2020.* Bogotá D.C. Recuperado el 24 de abril de 2021

16.2.3 ARTÍCULO DE PERIÓDICO

La República. (04 de mayo de 2020). Comercio electrónico ha crecido más de 300% en Latinoamérica en la pandemia. La República. Obtenido de https://www.larepublica.co/globoeconomia/e-commerce-ha-crecido-mas-de-300-en-latinoamerica-en-medio-de-la-pandemia-3000424

Pérez, V. (3 de octubre de 2019). La Superindustria ha impuesto 104 multas por mal manejo de datos personales. La República.

16.3 JURISPRUDENCIA

Corte Constitucional, (16 de octubre de 2008). Sentencia 1011 de 2008. *Revisión de Constitucionalidad del Proyecto de Ley Estatutaria N°27/06 Senad-221/07 Cámara (Acum.05/06 Senado) por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros*

países y se dictan otras disposiciones.MP. Jaime Córdoba Triviño. Obtenido de Relatoría: C-1011-08 Corte Constitucional de Colombia

Corte Constitucional, (6 de octubre de 2011). Sentencia C-748 de 2011. *Control constitucional al Proyecto de Ley Estatutaria N°184 de 2010 Senado, 046 de 2010 Cámara, por la cual se dictan disposiciones generales para la protección de datos personales.MP. Jorge Ignacio Pretelt Chaljub.* Obtenido de Relatoría*:* C-748-11 Corte Constitucional de Colombia

Corte Constitucional, (13 de mayo de 2015). Sentencia C-284 de 2015. Demanda de Inconstitucionalidad en contra del artículo 4° (parcial) de la Ley 153 de 1887. MP. Mauricio González Cuervo. Obtenido de Relatoría: C-284-15 Corte Constitucional de Colombia

Superintendencia de Industria y Comercio. Delegatura para la Protección de Datos Personales. (24 de enero de 2019) Resolución N°1321. Por la cual se imparten órdenes dentro de una actuación administrativa. Caso Facebook.

Superintendencia de Industria y Comercio. Delegatura para la Protección de Datos Personales. (18 de junio de 2019). Resolución N°21478. Por la cual se imparten órdenes dentro de una actuación administrativa. Caso Uber.

Superintendencia de Industria y Comercio. Delegatura para la Protección de Datos Personales. (05 de febrero de 2020). Resolución N°3344. Por la cual se resuelve un recurso de apelación. Caso Une Epm Telecomunicaciones.

Superintendencia de Industria y Comercio. Delegatura para la Protección de Datos Personales. (31 de julio de 2020). Resolución N°43704. Por la cual se resuelve un recurso de apelación. Caso Creditítulos, Cifin y Experian Colombia.

Superintendencia de Industria y Comercio. Delegatura para la Protección de Datos Personales. (07 de julio de 2021). Resolución N°41984. Por la cual se resuelve un recurso de apelación. Caso Avantel.

16.4 LEYES

Congreso de la República de Colombia. (31 de diciembre de 2008). Ley 1266. *Por la cual se dictan disposiciones generales del hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.*

Congreso de la República de Colombia. (17 de octubre de 2012). Ley 1581. *Por la cual se dictan disposiciones generales para la protección de datos personales.*

Congreso de la República de Colombia. (18 de agosto de 1999). Ley 527. *Por medio de la cual se define y reglamente 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.*

Congreso de la República de Colombia. (12 de octubre de 2011). Ley 1480 de 201*1, por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones.*

Presidencia de la República de Colombia. (27 de junio de 2013). Decreto 1377 *por el cual se reglamente parcialmente la ley 1581 de 2012. Derogado parcialmente por el Decreto 1081 de 2015.*

Presidencia de la República de Colombia. (26 de mayo de 2015). Decreto 1074. *Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.*