LEYES DE PROTECCIÓN DE DATOS PERSONALES: UNA RECOPILACIÓN NORMATIVA PARA ORIENTAR A EMPRESAS DE CONTACT CENTER EN EL CUMPLIMIENTO DE LAS LEYES DE PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA, ESTADOS UNIDOS Y EUROPA

Autora:
JULIETH CRISTINA GUTIÉRREZ RESTREPO

MONOGRAFÍA

Asesor:
MARIANA VILLEGAS GIRALDO

UNIVERSIDAD EAFIT
ESCUELA DE DERECHO
PREGRADO DE DERECHO
Abril de 2022
Medellín

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

RESUMEN

En el presente trabajo monográfico se pretende hacer un listado de las diversas normas que se han expedido alrededor del tema de protección de datos personales tanto en Colombia, como en el Estado de California en Estados Unidos y en la Unión Europea, con el fin de que las empresas que presten servicios de Contact Center puedan tener mayor certeza de aquellos aspectos normativos que debe tener en cuenta a la hora de prestar sus servicios, bien sea a clientes de origen nacional, o radicados en las regiones anteriormente mencionadas.

PROTECCIÓN DE DATOS PERSONALES, HABEAS DATA, DERECHO, PRIVACIDAD, RGPD, CCPA.

1. PRIMERA PARTE

1.1. INTRODUCCIÓN

La libertad de empresa es un derecho constitucional estipulado en el artículo 333[1] de la Constitución Política de Colombia, en el marco del bien común y las responsabilidades que conllevan el desarrollo y ejercicio del derecho, limitada sólo por la ley para el cuidado del interés social, la preservación del patrimonio cultural nacional y el medio ambiente. De acuerdo con la Corte Constitucional,

> *La intervención del Estado en la economía busca conciliar los intereses privados presentes en la actividad empresarial, con el interés general involucrado en el buen funcionamiento de los mercados para lograr la satisfacción de las necesidades de toda la población en condiciones de equidad y con el fin de conseguir el mejoramiento de la calidad de vida de los habitantes, la distribución equitativa de las oportunidades y los beneficios del desarrollo y la preservación de un ambiente sano.*[2]

La intervención que realiza el Estado sobre la economía en términos de la libertad de empresa se puede evidenciar en aspectos como el salario mínimo, los límites a la libre competencia y la protección de los datos personales.

Con la evolución tecnológica, surgen nuevos modelos de negocios, se expanden las capacidades de conexión entre personas y mercados, trascendiendo las fronteras nacionales e internacionales, lo que se da con la evolución además de la tecnología y la informática. Las personas, por necesidad o por voluntad,

---

[1] COLOMBIA. SECRETARÍA GENERAL DEL SENADO. Constitución Política de Colombia. Art. 333.
[2] CORTE CONSTITUCIONAL. Sentencia C-263/2011, 6 de abril de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

constantemente realizan transacciones para la consecución de bienes y servicios, muchas veces, de manera informal, otras implican que un usuario o comprador, provea de información personal que puede incluir su nombre, identificación, correo electrónico, números de teléfono, ideología, religión, inclinaciones políticas, etc. Si bien el Estado protege la libertad de empresa y los diversos derechos económicos que ello conlleva, estos derechos no pueden vulnerar en ningún momento los derechos fundamentales, el interés general y las buenas costumbres. Con respecto a la protección de los datos personales, también la Constitución Política señala en el artículo 15 el derecho de *habeas data* [3] . Sobre esto, la Corte Constitucional de manera reiterada lo ha conceptualizado como un derecho fundamental que habilita al titular de información personal a exigir, de la administradora de sus datos personales, que sean conocidos, actualizados, rectificados, suprimidos.[4]

A principios de los 90, Colombia empezó a convertirse en uno de los epicentros de un nuevo modelo de negocio globalizado conectando a otros sectores económicos con sus usuarios o consumidores de forma más eficaz e inmediata, llamando a las empresas, permitiendo que puedan conectarse con sus intereses, con la información, de manera personalizada. Este modelo de negocio, que se trabaja en la mayoría de sus veces en la modalidad de outsourcing, implica una transferencia de una gran cantidad de datos, que permite que las empresas de Contact Center, como proveedores, puedan acercarse a los clientes o usuarios de las empresas contratantes, y poder hacer esto, supone que los proveedores realicen su actividad comercial de manera satisfactoria, rentable y legal.

Es por eso que el propósito de este trabajo es brindar lineamientos, mostrar una guía de ruta, para que las compañías de Contact Center en Colombia, conozcan cómo pueden agregar valor a los servicios que prestan, por medio de la información organizada y concisa sobre la normatividad vigente, realizando un

---

[3] Op Cit. Art. 15.
[4] CORTE CONSTITUCIONAL. Sentencia T-176A/14, 25 de marzp de 2014. Magistrado Ponente: Jorge Ignacio Pretelt Chaljub.

acercamiento de las normas vigentes alrededor del problema de la protección de datos personales en Colombia, Estados Unidos y Europa.

1.2. JUSTIFICACIÓN

Reconociendo el carácter novedoso y riguroso que caracteriza a las normas de protección de datos personales, y que su infracción impone a las empresas en general, pero para efectos de este proyecto, las de Contact Center, multas excesivamente altas, resulta imperativo realizar una recopilación de las principales regulaciones que al respecto han hecho la Unión Europea, Estados Unidos y Colombia, y con ello, aportar certeza y orientar sobre los aspectos que se deben tener en cuenta al momento de celebrar negocios jurídicos con organizaciones que deban observar las leyes de los lugares mencionados, y también, para el desarrollo de sus propios negocios o actividades comerciales, de modo tal, que este trabajo, sirva a las empresas como una guía para capacitar al personal sobre la normatividad protección de datos personales en cada legislación, según sea necesario para el desenvolvimiento exitoso de sus negocios, y les sea posible continuar con la enseñanza a medida que surjan nuevas actualizaciones normativas y así dar una cobertura amplia y segura a la salvaguarda de los datos personales, que son clave fundamental para el desarrollo de los negocios de los centros de contacto.

1.3. OBJETIVOS

1.3.1. Objetivo General

Construir una guía de sobre la normatividad protección de datos personales en Colombia, Estados Unidos y la Unión Europea y recopilarlas con el fin de describir las obligaciones adquiridas dentro de la responsabilidad sobre el

tratamiento de los datos, y del encargado de su tratamiento, para aportar certeza a las empresas de Contact Center a cerca de los aspectos normativos que debe tener en cuenta para el normal desarrollo de sus negocios.

1.3.2. Objetivos Específicos

- Analizar la importancia de la protección de datos personales a la luz de la legislación colombiana y la historia.
- Compilar las obligaciones que tienen sobre todo los encargados del tratamiento de datos personales según la ley de Colombia.
- Enumerar las sanciones que contemplan las autoridades de Colombia respecto a la violación de las leyes de datos personales.
- Estudiar las leyes de protección de datos personales en Estados Unidos y la Unión Europea.
- Compilar las obligaciones que tienen sobre todo los encargados del tratamiento de datos personales según las leyes de Estados Unidos y la Unión Europea.
- Enumerar las sanciones que contemplan las legislaciones de Estados Unidos y la Unión Europea con respecto a la violación de las leyes de datos personales.

2. SEGUNDA PARTE

2.1. LA INDUSTRIA DE CONTACT CENTER EN COLOMBIA

Los servicios de Contact Center se han prestado en Colombia, en su mayoría, bajo la modalidad de outsourcing, conociéndose este sector hoy en día como BPO, que comprende servicios como servicio al cliente, televenta, consultoría, análisis de datos, cobranzas, a través del Contact Center. Este modelo de negocios llegó a Colombia en los años 90, con una firma internacional española, denominada Indra, y se ha venido posicionando en el país con clientes nacionales, pero también, con potenciales clientes en España y Estados Unidos.

Según la Asociación colombiana de BPO, este sector ha generado empleo a más de 250.000 personas, y que esto es así, porque Colombia es un país que brinda estabilidad jurídica para que las compañías puedan invertir en las empresas nacionales, como una oportunidad para crecer e incursionar en nuevos mercados a nivel nacional e internacional ofreciendo precios competitivos, disponibilidad de talento humano, para exportar servicios de alta calidad incorporando nuevas tecnologías digitales.

En palabras de Ana Karina Kessep Alcove, actual presidente ejecutiva de la Asociación Colombiana de Bussiness Processes Outsourcing, *"Las bases de datos pasaron de ser manejadas en archivos de Excel, complejos y desordenados, a utilizar tecnología de última generación con capacidades predictivas, que hacen más exactos, ordenados y rigurosos los procesos."*[5], lo que permite inferir que uno de los activos más importantes de estas organizaciones son las bases de datos, que, en estos contratos, se realiza

[5] PORTAFOLIO. La profesionalización de los Contact Center. 20 de Junio de 2016. En: Revista Portafolio [Online]. https://www.portafolio.co/evolucion-contact-centers-colombia-revista-portafolio-497791

transferencia de datos personales de usuarios y consumidores ya sean actuales de los clientes o futuros que se comuniquen con los centros de contacto, es por esto, que las empresas del sector requieren seguir creciendo y para eso, deben capacitar a sus empleados en las mejores técnicas y prácticas laborales. Teniendo en cuenta la importancia que tienen las bases de datos para las compañías de Contact Center, hay una serie de estándares que ellas deben seguir y existen varios tipos de certificaciones que sirven como garantía de que los servicios prestados efectivamente son de calidad. Algunas de estos estándares son ISO 9001, que evalúa el sistema con la que la empresa gestiona sus prácticas de calidad en función de sus clientes, la forma en que se desarrollan sus negocios, su manejo del talento humano, su infraestructura tecno-física. Igualmente, la ISO 27001 está focalizada sobre el sistema de gestión de la seguridad informática y de la información, que es el activo más valioso tanto de las compañías contratantes como de los proveedores que serían quienes presten los servicios de Contact Center. Y Certificación COPC orientada a los servicios de Contact Center, con alcance internacional, que busca la optimización de la experiencia de clientes.

Pues bien, como afirma la Asociación Colombiana de BPO, uno de los atractivos de las compañías de Contact Center en Colombia es la estabilidad jurídica, eso significa que las empresas deban cumplir con todo lo que exige la ley para el efecto, lo que conlleva a que cada vez sean más las compañías internacionales que buscan la atención de sus clientes a través de Contact Center colombianos. Para efectos del presente trabajo monográfico, se ahondará en las leyes encargadas de la protección de datos personales tanto en Colombia, pero también en lo que deben cumplir las compañías colombianas cuando se trate de clientes en localizados en Europa y Estados Unidos.

2.2. IMPORTANCIA DE LA PROTECCIÓN DE DATOS PERSONALES EN EL CASO COLOMBIANO

El *habeas data,* derecho consagrado en el artículo 15 de la Constitución Política[6] ha pasado por un proceso para ser constituido como derecho en el ordenamiento jurídico Colombiano. La Ley 23 de 1981, en su artículo 34, le otorgó privacidad a los datos registrados en la historia clínica, mencionando que el registro de la misma sólo lo pueden conocer terceros en los casos en los que el paciente lo autorice o según lo que especifique la ley, estos datos es lo que conocemos el día de hoy como datos sensibles según el artículo 5 de la Ley 1581 de 2012, y lo consagrado en el artículo 34 de la Ley 23 de 1981, fue regulado más adelante en la Resolución 1995 de 1999 del Ministerio de Salud, a través del artículo 14. En el ordenamiento actual, marcado por el artículo 15 de la Constitución Política, se estipula que las personas tienen derecho al pleno conocimiento, actualización y rectificación de la información que se haya recolectado de ellas en bases de datos o archivos ya sea de carácter público o privado, pero el artículo por sí solo, no da el alcance o el entendimiento que este derecho requiere[7], por lo que más adelante, el Congreso de la República expide la Ley 1266 de 2008, posteriormente la Ley 1581 de 2012 y reglamentada más adelante por el Decreto 1377 de 2013, y actualmente, es la Superintendencia de Industria y Comercio la delegada para la vigilancia del cumplimiento de esta normatividad.

A pesar de que a la fecha han transcurrido varios años tras la actualización y entrada en vigor de las normas anteriormente mencionadas, aún no ha habido una certeza a ciencia cierta de lo que las compañías, en el sector privado, y para efectos del presente trabajo, en el sector de Contact Center, deben cumplir para la protección de derechos de aquellas personas naturales poseedoras de los datos. Esto resulta crucial, teniendo en cuenta la forma en la que trabajan estas empresas, puesto que, a diario, tienen contacto con usuarios y consumidores, que otorgaron sus datos con anterioridad o que los proporcionan de manera posterior al hacer contacto con los Contact Center y que, las sanciones por la violación a la normatividad pueden ser altamente onerosas. Este tipo de

[6] CONSTITUCIÓN POLÍTICA DE COLOMBIA. Op. Cit. Art 15.
[7] Ibid

incertidumbre, no sólo genera riesgos para los usuarios y consumidores, sino también para los contratantes y para las empresas que proveen estos servicios.

La irrupción de la emergencia sanitaria relacionada con la pandemia de Covid-19, llevó a que las empresas de Contact Center trabajaran de manera incansable, a pesar de todas las limitaciones para la movilidad y de las restricciones respecto de las personas que concurren en un espacio, aun así, era el tipo de negocio que se necesitó que continuara en ejecución, puesto que, los usuarios y consumidores, necesitaban poder contactar a las compañías de manera directa, personal e inmediata, no habiendo otros modos de poder resolver sus inquietudes o requerimientos. Esto permite concluir, que no son sólo los avances tecnológicos los que permiten que los datos se transen de forma nacional e incluso internacional, sino que las circunstancias coyunturales también se vuelven en una razón de peso para que este tipo de negocios continúe prosperando, y que, por tanto, se siga desarrollando la dirigida a regular el tratamiento de los datos personales.

La ignorancia sobre las obligaciones que recaen sobre las empresas respecto del tratamiento de datos, o la incorrecta aplicación de las normas dentro de sus actividades diarias, pueden acarrear sanciones multimillonarias e incluso, el cierre del establecimiento de comercio; no tener conocimiento de la ley sobre la materia jurídica, no brinda estabilidad jurídica a los usuarios, consumidores ni a las empresas que contratan el servicio de Contact Center, además de que impide el crecimiento de las empresas que prestan estos servicios; pues bien se sabe que *"ignorantia juris non excusat"* o *"la ignorancia de la ley no sirve de excusa"*, y así lo asevera la Corte Constitucional al afirmar que:

> *"es necesario exigir de cada uno de los miembros de la comunidad que se comporte como si conociera las leyes que tienen que ver con su conducta. La obediencia al derecho no puede dejarse a merced de la voluntad de cada uno, pues si así ocurriera, al mínimo de orden*

que es presupuesto de la convivencia comunitaria, se sustituiría la anarquía que la imposibilita"[8]

Por esta razón, las empresas de Contact Center deben estar informadas sobre la normatividad actual aplicable alrededor de la protección de datos personales y capacitar a todo su personal pertinente para el efecto, y así contribuir a la tranquilidad de los ciudadanos con los que tengan contacto y al crecimiento empresarial y laboral.

2.3. NORMATIVIDAD APLICABLE A LA PROTECCIÓN DE DATOS PERSONALES EN LA LEGISLACIÓN COLOMBIANA

Teniendo en cuenta lo anteriormente expuesto, en Colombia se puede aplicar una serie de normas directamente relacionadas con la protección de datos personales que deben ser tenidas en cuenta por las compañías que presten servicios de Contact Center.

- La Ley 1266 de 2008, es la relacionada a la operacionalización del *habeas data* en sus disposiciones generales. Regula el manejo de la información contenida en bases de datos personales, la proveniente de otros países, entre otros temas relacionados.
- La Ley 1273 de 2009, modifica el Código Penal, crea el nuevo bien jurídico tutelado *"protección de la información y de los* datos".
- El Decreto 1727 de 2009, que determina la forma en la cual en la que los operadores de bancos de datos de información proveniente de terceros países, entre otros, deben presentar la información de los titulares de la información.

---

[8] CORTE CONSTITUCIONAL. Sentencia C-651 del 3 de diciembre de 1997. Magistrado Ponente Carlos Gaviria Díaz

- La Ley 1581 de 2012, dicta disposiciones generales para la protección de datos personales, *habeas data.*
- El Decreto 1377 de 2013, reglamenta la Ley 1581 de 2012.
- La Circular Única, título V, de la Superintendencia de Industria y Comercio.
- El Decreto 886 de 2014, reglamenta el artículo 15 de la Ley 1581 de 2012.
- El Decreto 1074 de 2015, reglamenta el sector comercio, industria y turismo.
- La Ley 1928 de 2018, aprueba y adapta para Colombia el Convenio sobre la ciberdelincuencia desarrollado el 23 de noviembre de 2001 en Budapest.

La Ley 1266 de 2008 y el Decreto 1727 de 2009, hacen referencia directa a las bases de datos sobre información financiera, que no sería materia como tal para las compañías de Contact Center, aunque sí para sus clientes, en este sentido, se recomienda que las empresas que proveen servicios de Contact Center, que en adelante denominaremos “PROVEEDOR” (con el fin de comprender el destinatario de las obligaciones y sanciones que se enunciarán), en sus contratos, añadan cláusulas en las cuales los “CLIENTES” (que pueden ser entidades del sector financiero) tengan la obligación de informar y actualizar al PROVEEDOR en la normatividad que les aplique, para que de esta forma, toda sanción por incumplimiento en los temas de especialidad de los CLIENTES, sean atribuibles a estos directamente por la insuficiencia de la información otorgada y no al PROVEEDOR.

En cuanto al contenido de la Ley 1266 de 2008, dentro de esta se consigna una lista de las obligaciones que debería tener en cuenta el PROVEEDOR a la hora de prestar sus servicios, al igual que, de las posibles sanciones que acarrearía el incumplimiento de las mismas, y así, el PROVEEDOR y su personal, pueda estar informado y proveer estabilidad jurídica a sus CLIENTES, a nivel nacional e internacional.

Para efectos del presente trabajo, se tendrán en cuenta las siguientes definiciones:

Titular de la información: Es cualquier persona natural o jurídica a la que se puede atribuir la información existente en los bancos de datos, por lo tanto constituye el sujeto del derecho de *habeas data* y todos los derechos y garantías que le confiere la ley como dueño de los datos.[9]

Fuente de información: Es cualquier persona, entidad u organización que conoce o recibe datos de los titulares. Normalmente esto se realiza en el marco de una relación comercial o prestación de un servicio, aunque puede ser de cualquier otra índole, siempre a través de autorización legal o del titular. Estos datos normalmente van hacia el operador de información, que a su vez los transmite al usuario final. Si la fuente entrega de manera directa la información a los usuarios y no a través de un operador, también tendrá la condición de operador y asumirá sus deberes y responsabilidades. La fuente de la información responde por la calidad de la información proporcionada al operador pues debe cumplir con los deberes y responsabilidades previstos para garantizar la protección de los datos del titular.[10]

Operador de información: Persona, entidad u organización que recibe de la fuente datos personales de diversos titulares. Su función normalmente es administrar y poner en conocimiento de los usuarios estos datos bajo parámetros legales. Al tener acceso a la información personal de terceros, adquiere deberes y responsabilidades respecto a la protección de los datos de todos los titulares. En caso de que el operador no sea a su vez la fuente de información, el operador no tiene relación comercial o de servicio con el titular, por lo que no es necesario que responda por la calidad de los datos que se le hayan proporcionado.[11]

---

[9] CONGRESO DE LA REPÚBLICA. Ley 1266 de 2008, artículo 3, literal a.
[10] Ibid. Lit b.
[11] Ibid. Lit c.

Usuario: Persona natural o jurídica que puede acceder a la información de uno o varios de los titulares, según la ley lo permita y de los modos en que lo permita. Accede a la información suministrada bien sea por la fuente o por el operador, o de manera directa por el titular de la información. Al tener el usuario acceso a la información de algún titular, debe garantizarle los deberes y responsabilidades propios de la protección de sus datos personales.[12].

Dato público: Considerado así según lo dispuesto en la Constitución Política o en la ley, y los datos que no sean privados o semiprivados. También se consideran así, los datos relativos a la profesión u oficio, en calidad de comerciante o servidor público contenidos en cualquier fuente no sometida a reserva.[13]

Dato semiprivado: Es cualquier dato que no tiene naturaleza íntima, o reservada o pública. El conocimiento o divulgación de este puede interesar no solo a su titular sino a algún sector o grupo. Por ejemplo, los datos financieros de cualquier actividad comercial.[14]

***Dato privado*:** Es cualquier dato que por naturaleza es reservado o íntimo y que sólo es relevante para su titular.[15]

***Dato personal*:** Es el nombre que recibe toda información vinculada o que pueda asociarse a una o varias personas naturales o jurídicas, determinadas o determinantes.[16]

---

[12] Ibid.,Lit d.
[13] PRESIDENCIA DE LA REPÚBLICA. Decreto 1377 de 2013, artículo 3, numeral 2.
[14] Ibid., Lit g.
[15] Ibid., literal h.
[16] CONGRESO DE COLOMBIA. Ley 1581 de 2012, artículo 3, literal c.

Encargado del tratamiento: Persona natural o jurídica, privada o pública que realice el tratamiento de datos personales por cuenta del Responsable del Tratamiento, ya sea por sí misma o con interposición de otras personas.[17]

Responsable del tratamiento: Es la Persona natural o jurídica pública o privada que toma decisiones sobre la base de datos y/o el tratamiento de los datos.[18]

Tratamiento: Se denomina así a cualquier operación o conjunto de operaciones de recopilación, almacenamiento, procesamiento, circulación, supresión o uso.[19]

Datos sensibles: Son todos aquellos que afectan la intimidad del titular. El manejo y tratamiento de estos datos tiene fuertes connotaciones éticas pues si se usan indebidamente pueden generar discriminación o amenazar la seguridad de la persona. Esto puede incluir pero no limitarse a raza o etnia, inclinación política, creencias religiosas o posturas filosóficas, así como la pertenencia a sindicatos u organizaciones sociales, de derechos humanos, la salud, la vida sexual y los datos biométricos.[20]

Registro Nacional de Bases de Datos: Es el directorio público de las bases de datos sujetas a tratamiento dentro del país. Este registro es administrado por la Superintendencia de Industria y Comercio, deben registrarse todos los actores involucrados en la gestión de datos los cuales darán cuenta de sus políticas de tratamiento de datos.[21]

Aviso de privacidad: Es toda comunicación verbal que el titular recibe del responsable del tratamiento de datos donde es informado acerca de qué

---

[17] Ibid, literal d.
[18] Ibíd, literal e.
[19] Ibíd, literal g.
[20] Ibid Art. 5.
[21] Ibid,Art.25.

tratamiento tendrán y cuáles son las políticas que determinan estos procesos, al igual que cómo podrá tener acceso a ella y cuál será su finalidad.[22]

Transferencia: Se da en los escenarios en que el Responsable o Encargado del tratamiento de los datos envían la información a un receptor dentro o fuera del país, tomando Colombia como punto de origen. El receptor actuará a su vez como Responsable.[23]

Transmisión: Se refiere a la a la comunicación que se hace de los datos personales, como consecuencia del tratamiento, dentro o fuera del país.[24] Si se hace fuera del país, para que el Encargado realice el tratamiento por encargo del Responsable, no será necesario que se informe al Titular, ni que, el Titular dé su consentimiento.[25]

Estas anteriores definiciones deben permitir a las empresas del sector de Contact Center comprender el tipo de procesos y responsabilidad que existe al respecto, considerando que estas manejan una voluminosa movilidad de datos de un país a otro. Para esto, se propone identificar los siguientes principios, que a su vez son compartidos con el Reglamento General de Protección de Datos de la Unión Europea (en adelante, RGPD)[26].

1. ***Veracidad y calidad de los datos:*** La información que se trate, debe ser completa, veraz, exacta, actualizada, comprensible y comprobable; no se permitirá el registro o divulgación de información parcial, incompleta, fraccionada o que induzca a error.[27] Esto, comparándolo con el RGDP,

[22] Op Cit. Decreto 1377, Art. 3, numeral 1.
[23] Ibid, numeral 4.
[24] Ibid, numeral 5.
[25] Ibid, artículo 24.
[26] UNIÓN EUROPEA. Reglamento General de Protección de Datos. 24 de mayo de 2018
[27] Op. Cit. Ley 1266. Art. 4. Lit a.; Ley 1581, Art. 4, lit f.

aparece en este como Principio de Exactitud, que además añade que los datos inexactos deben suprimirse o rectificarse.[28]

2. ***Finalidad:*** El tratamiento de la información tiene una finalidad y esta debe ser efectuada de manera legítima, informando previamente al titular y sujeto a la autorización que este dé sobre el proceso.[29]
3. ***Circulación Restringida:*** El tratamiento de los datos debe sujetarse a los límites derivados de la naturaleza de los datos, de lo dispuesto por la ley y de los principios de la administración de datos personales, en especial el de finalidad y el de temporalidad. Los datos personales, a diferencia de la información pública, no deben ser accesibles por internet o por otros medios de divulgación o comunicación masiva, a no ser de que el acceso sea controlable técnicamente para brindar un conocimiento sólo a los titulares o los usuarios autorizados de acuerdo a la ley.[30]
4. ***Temporalidad:*** Los datos deben ser de disponibilidad temporal, es decir, cuando dejan de servir a la finalidad para la que se recolectaron, no se podrá suministrar la información del titular a usuarios o terceros.[31] Al compararse con el RGPD, este contempla la posibilidad de que, si son datos de interés público, se puedan conservar por más tiempo para investigaciones científicas, estadísticas e históricas.[32]
5. ***Interpretación Integral de Derechos Constitucionales:*** Las disposiciones de la Ley 1266 de 2008, en la hermenéutica jurídica de cada caso, debe interpretarse girando alrededor de la protección de los derechos constitucionales, concretamente el *habeas data,* y a su vez el derecho a la honra, la intimidad, el buen nombre, y el derecho a la información.[33] Sobre este último, se consagra en el artículo 20 de la Constitución Política.[34]

---

[28] Op Cit. Reglamento General de Protección de Datos. Art. 5. Lit. d.
[29] Íbid.
[30] Op Cit. Ley 1266. Art. 4, Lit. c.
[31] Ibid Lit. d.
[32] Op. Cit. RGDP. Art. 5. Lit e.
[33] Ibid. Lit e.
[34] Op. Cit. Constitución Política de Colombia. Art. 20.

6. ***Seguridad:*** El principio de seguridad obliga a que toda la información manipulada en los bancos de datos y que resulta de las consultas que los usuarios realicen, deben poseer las medidas técnicas necesarias para garantizar la seguridad de los registros contra su pérdida, adulteración, o consultas o usos no autorizados[35].
7. ***Confidencialidad:*** Todos los datos no públicos deben ser datos reservados, para lo cual este principio obliga a las personas naturales y jurídicas que administren los datos personales guardar reserva de la información en todo momento, incluso habiendo finalizado cualquier labor de manejo de los datos. Estos actores tienen la facultad de realizar suministro o comunicación de los datos si corresponden al desarrollo de sus actividades autorizadas por la Ley 1266 de 2008.[36]
8. ***Favorecimiento a una actividad de interés público:*** Este principio, el cual más que todo se refiere a la actividad sobre los datos en el sector financiero y la información proveniente de terceros países, exhorta a que la administración de la información se produzca buscando favorecer los fines de expansión y democratización del crédito, considerando la actividad financiera como un interés público, lo que hace que los usuarios de la información no puedan basarse en la información negativa del titular para tomar decisiones sobre solicitudes crediticias.[37]
9. ***Legalidad en materia de tratamiento de datos personales:*** De acuerdo con este principio, se dispone que todo tratamiento de datos personales es una actividad con regulación por parte de la ley y debe sujetarse en todo momento a lo que esta y sus normas establezcan.[38]
10. ***Libertad:*** Desde este principio, los tratamientos de datos deben efectuarse exclusivamente bajo el consentimiento informado, expreso y previo de los titulares.[39]

---

[35] Op. Cit. Ley 1266. Art. 4. Lit. f. Ley 1581. Art. 4. Lit. g.
[36] Ibid.
[37] Ibid. Art. 10.
[38] Op. Cit. Ley 1581. Art. 4.
[39] Ibid. Lit. C.

11. ***Transparencia:*** Por último, este principio radica en que debe garantizarse para el titular el derecho de obtener información alrededor de la existencia de datos que le conciernen directamente, sin limitaciones ni restricciones, aspecto que debe ser protegido tanto por quienes fungen como Encargados y como Responsables.[40]

2.3.1. Obligaciones alrededor del tratamiento de datos.

1. El PROVEEDOR debe garantizarle al titular de la información la posibilidad de ejercer sus derechos al *habeas data* y de petición (Ley 1266 de 2008, artículo 7, numerales 1, 7, 8 y Ley 1581, artículo 17, literal a).

- El titular de la información debe poder conocer la información que exista de él en los bancos de datos, ello implica que el PROVEEDOR o el CONTRATANTE, le brinden la información que solicita el titular, teniendo en cuenta los principios ya mencionados, entre ellos, que la información sea veraz.
- El PROVEEDOR quien es el encargado de administrar los datos a petición del CONTRATANTE, deberá actualizar y corregir los datos cuando así lo solicite el titular.
- También, deberá dar el trámite establecido por ley a las consultas, peticiones o reclamos que realice el titular de los datos.

De igual forma, tanto el PROVEEDOR como el CONTRATANTE deberán implementar un manual interno de políticas y procedimientos sobre la administración de datos, con el fin de garantizar el cumplimiento adecuado de las leyes para el efecto, y para dar el trámite debido a las consultas, peticiones o reclamos que hagan los titulares. (Ley 1266 de 2008, artículo 7, numeral 4 y Ley 1581 de 2012, artículo 17, literal k, artículo 18, literal f). Las políticas deben constar en medio físico o electrónico, con lenguaje claro, y sencillo, y deben

[40] Ibid.

ponerse a disposición de los titulares; ellas deben contener por lo menos, los datos de identificación del Responsable (nombre o razón social, domicilio, dirección, correo electrónico y teléfono), cómo serán tratados los datos y con qué finalidad, los derechos que tienen los titulares, la persona o el área encargada de atender las peticiones, quejas o reclamos, el procedimiento para que los titulares puedan hacer efectivo el goce de sus derechos, fecha entrada en vigencia de la política y periodo de vigencia de la base de datos (Decreto 1377 de 2013, artículo 13).

En caso de que no sea posible poner a disposición del Titular la política de tratamiento de datos, se le debe informar mediante un aviso de privacidad sobre la existencia de esas políticas y de qué forma puede acceder a ellas. El aviso de privacidad debe contener la identificación del Responsable, cómo serán tratados los datos y con qué finalidad, los derechos que tienen los titulares y los mecanismos que tienen para conocer la política de tratamiento de datos; cuando se traten de datos sensibles, se debe expresar el carácter facultativo de la autorización de tales datos. Sin embargo, esto no exime el deber de dar conocer la Política al titular. (Decreto 1377 de 2013, artículos 14 y 15).

Recomendación: En este sentido, se recomendaría que el PROVEEDOR haga un reporte de manera inmediata al momento en que reciba una petición o requerimiento del titular respecto de la información para que sea el CONTRATANTE quien se encargue de dar respuesta en los términos establecidos por la ley para el derecho de petición. Sin embargo, en los casos en los que el CONTRATANTE encargue al PROVEEDOR dar trámite a los derechos de petición de los titulares respecto de su información, se recomienda que el PROVEEDOR cuente con personal idóneo para responder en los términos legales y evitar sanciones, o capacitar a su personal para el efecto.

Adicional a ello, sin tener experticia en el área tecnológica, sería recomendable que el PROVEEDOR cuente con una plataforma que le permita escalar los requerimientos de los titulares y segmentarlos de acuerdo a los temas de que

traten, y que la plataforma les permita a los asesores encargados de tramitar el requerimiento y a sus jefes, recibir alertas antes del vencimiento.

Es necesario que el PROVEEDOR, realice una revisión de las políticas contenidas en los manuales para la protección de datos personales y para la seguridad de la información, hacer pruebas a los planes que contengan de manera periódica, sería prudente realizarlo por lo menos dos veces al año, o con una periodicidad prudente, y efectuar evaluaciones de riesgos, con el fin de dar garantía y seguridad a sus clientes y anticipar las auditorías que le realicen estos últimos o los entes de certificación.

2. Tanto el PROVEEDOR como el CONTRATANTE deben dar cumplimiento al principio de confidencialidad, y garantizar que sólo las personas que tengan autorización por parte de la ley tengan acceso a la información brindada por el titular. (Ley 1266 de 2008, artículo 7, numeral 3 y Ley 1581 de 2012, artículo 17, literal d, artículo 18, literal b).

El PROVEEDOR debe garantizar que el lugar en el que se almacenen los datos de los titulares sea seguro, e impedir que se deterioren, que sufran pérdidas, se alteren, sean usados sin autorización o de manera fraudulenta; en los casos en los que los conserve para tu administración y tratamiento. (Ley 1266 de 2008, artículo 7, numeral 6).

Recomendación: Es importante que el CONTRATANTE sea quien se asegure de que la modalidad y forma escogida para transmitir los datos personales al PROVEEDOR sea segura, de esta forma, este último se eximiría de cualquier fuga en el momento de la transmisión, aun así, el PROVEEDOR, debe garantizar que se mantengan confidenciales los datos durante el tiempo que dure la relación comercial entre las partes, por lo que se debe asegurar de implementar los controles y la seguridad necesaria tanto en sus instalaciones como en su infraestructura tecnológica, ello implica que el personal pueda conocer cómo proteger la confidencialidad y además, suscribir acuerdos de confidencialidad y

explicarles los alcances que puede tener su infracción; además, es necesario que el PROVEEDOR aplique las mismas medidas que debe ejercer él mismo, a sus proveedores, en los casos en que tengan acceso a los datos de los titulares, o que por alguna razón, los puedan llegar a conocer.

3. La fuente debe contar con prueba de la autorización otorgada por el titular para proceder al tratamiento de sus datos, en los casos en que la ley lo requiera. (Ley 1266 de 2008, artículo 7, numeral 5 y Ley 1581 de 2012, artículo 17, literal b). Sin embargo, la autorización no será necesaria cuando sea requerida por una entidad pública o administrativa en ejercicio de funciones legales o judiciales, cuando sean de naturaleza pública, en casos de urgencia o emergencia médica o sanitaria, cuando sea para fines históricos, científicos o estadísticos, de acuerdo a la ley y los datos del estado civil de las personas (Ley 1581 de 2012, artículo 10).

Al momento de solicitar la autorización se debe informar al titular sobre el tratamiento que se le darán a sus datos y la finalidad con la que serán tratados, el carácter facultativo de sus respuestas cuando trate de datos sensibles, de niños, niñas y adolescentes, sus derechos como titular, y la identificación del Responsable, junto con dirección física o electrónica y teléfono de contacto. (Ley 1581 de 2012, artículo 12, artículo 17, literal c). Se debe garantizar al menor el derecho de ser escuchado, su opinión podría ser valorado dependiendo de su madurez, autonomía y capacidad para entender (Decreto 1377 de 2013, artículo 12).

<u>Recomendación:</u> Una de las formas que tiene el PROVEEDOR de protegerse o de alguna manera, librarse de esta obligación de alguna forma, es en la etapa pre-contractual con sus clientes, en los momentos en los que se estén acordando las condiciones para la ejecución del contrato y en el momento en el que se estén concertando las cláusulas contractuales, para que, quede claro que la empresa CONTRATANTE será la que se encargue de contar con la prueba de la autorización otorgada por el titular cuando ello implique la transmisión de datos

personales. De todas formas, es posible que el PROVEEDOR recolecte datos personales en las diversas formas de comunicación que actualmente existen, ya sea de manera telefónica, por mensaje de texto, vía WhatsApp, correo electrónico, y atendiendo a la calidad de los datos, es necesario que el PROVEEDOR recolecte de manera correcta estos datos, el titular otorgue la autorización para el tratamiento de sus datos, obtener la prueba de esta autorización y conservarla durante el tiempo que dure la relación comercial, o lo que hayan pactado las partes, y mientras subsistan los fines para los cuales fueron recolectados.

4. En el momento en que el titular de la información solicite que sus datos sean actualizados o deban ser rectificados, se debe indicar en el registro que sus datos se encuentran en discusión por parte del titular, hasta que este procedimiento se lleve a cabo completamente (Ley 1266, artículo 7, numeral 9). Adicionalmente, la fuente de la información, debe actualizar mensualmente la información que proporciona al operador. (Ley 1266 de 2008, artículo 12). Cuando el titular solicite la actualización de sus datos, deberá efectuarse dentro de los cinco (5) días hábiles siguientes a la fecha en la que se recibió la solicitud (Ley 1581 de 2008, artículo 18, literal d).

Recomendación: Es conveniente que se capacite al personal que se encargará del tratamiento de la información, para que, en estos casos, tengan en cuenta hacer la anotación sobre los datos en discusión, con el fin de que no se cometan errores que puedan causar molestias y desconfianza a los titulares de la información, y posibles quejas o requerimientos por lo mismo. También es recomendable, contar con un sistema que permita hacer el registro de la solicitud del titular para efectuar la actualización de su información, que impida que se elimine la solicitud hasta que haya sido completada, además de que genere alertas para dar solución antes de los días establecidos para ello.

5. La fuente de la información, es decir, EL CLIENTE, debe cumplir con varios requisitos:

- Garantizar que la información que proporciona sea veraz, completa, actualizada y comprobable. (Ley 1266 de 2008, artículo 8, numeral 1 y Ley 1581 de 2012, artículo 17, literal e, artículo 18, literal a).
- Reportar las novedades de los datos que proporcione de manera periódica y oportuna. (Ley 1266 de 2008, artículo 8, numeral 2 y Ley 1581 de 2012, artículo 17, literal f).
- En caso de que la información sea incorrecta, debe rectificarla e informarlo al PROVEEDOR. (Ley 1266 de 2008, artículo 8, numeral 3 y Ley 1581 de 2012, literal g).
- Solicitar y conservar copia o evidencia de la debida autorización (Ley 1266 de 2008, artículo 8, numeral 5, Decreto 1377 de 2013, artículo 8). Además, debe certificar semestralmente que la información proporcionada cuenta con tal autorización (Ley 1266 de 2008, artículo 8, numeral 6).
- Informar al proveedor en los casos en los que la información del titular se encuentre en discusión para el PROVEEDOR incluya dicha anotación en sus bancos de datos hasta que culmine. (Ley 1266 de 2008, artículo 8, numeral 8).

Recomendación: Es importante que, al momento de suscribir, ya sea el contrato de prestación de servicios, o el contrato de transmisión de datos personales, se puedan tener en cuenta estos aspectos, y, sobre todo, solicitar la certificación por parte del CLIENTE sobre la autorización de los datos, puesto que, la debida diligencia, llevará a las compañías de este sector a que su servicio se pueda desarrollar con continuidad y confiabilidad, esto es recomendable aun si el CLIENTE no es del sector financiero.

6. La ley impone el deber a los usuarios de dar prevalencia al principio de favorecimiento a una actividad de interés público, por lo que las compañías no pueden basarse exclusivamente en la información negativa del titular para acceder a un crédito. Sin embargo, vemos en la realidad, que, al momento de realizar solicitudes de crédito, y en los casos en los que es rechazada tal solicitud, la mayoría informa que las razones son reservadas o confidenciales; atendiendo

a este principio, podría decirse que el titular tiene el derecho a que se le informen cuáles son las razones por las cuales su solicitud es rechazada, con el fin de comprobar que sus derechos no han sido vulnerados. (Ley 1266 de 2008, artículo 10).

Por otro lado, sobre el reporte de información negativa, se debe seguir un procedimiento expreso para ello, antes de realizar el reporte, se debe enviar un comunicado a la última dirección del domicilio del titular, con el fin de darle la oportunidad de demostrar el pago o de otro modo efectuarlo; si en veinte (20) días no se ha resuelto la situación, se podrá realizar el reporte negativo a los operadores de bancos de datos de información financiera (Ley 1266 de 2008, artículo 12).

Recomendación: En medio de las operaciones, y a la hora de establecer el modelo de negocio con los CLIENTES, es importante tomar esto en cuenta, si el PROVEEDOR se encargará de estudios crediticios o lo que pueda relacionarse, para evitar incurrir en acciones que puedan acarrear sanciones a ambas partes.

7. Los operadores de la información deben cumplir varios requisitos, entre ellos, tener un área para la atención de peticiones, quejas y reclamos; tener un sistema de seguridad que garantice la seguridad y actualización de la información y actualizar la información reportada por la fuente en un tiempo inferior a diez (10) días calendario. (Ley 1266 de 2008, artículo 11).

8. Sobre las consultas, o peticiones, se debe contar con evidencia de ello por medios técnicos, y deberán ser atendidas dentro de los diez (10) días hábiles siguientes, a partir de la fecha en la que se recibió; si no es posible atenderla en ese tiempo, se deberá informar al solicitante expresando los motivos de la demora, y en todo caso, no podrá tardarse más de cinco (5) días hábiles siguientes al vencimiento del primer término. (Ley 1266 de 2008, artículo 16, numeral 1 y Ley 1581 de 2012, artículo 14). Respecto de los reclamos, y en caso de que la solicitud tenga fallas, se deberá informar al titular para que las subsane,

y tendrá un mes para hacerlo, si pasado este tiempo, el solicitante no ha proporcionado la información requerida, se entenderá que desistió de la solicitud. Máximo, dentro de los dos (2) días hábiles de recibida la solicitud, se debe adicionarle la leyenda “reclamo en trámite”, entre tanto se decide.

El operador tendrá máximo dos (2) días hábiles para trasladar la petición o reclamo y para anotar la leyenda sobre “reclamo en trámite” en sus registros., y el reclamo se deberá atender en quince (15) días hábiles a partir de la fecha en la que se efectuó la reclamación, y sólo podrá prorrogarse por ocho (8) días hábiles más. (Ley 1266 de 2008, artículo 16, numeral 2). Sin embargo, para los casos establecidos por la Ley 1581 de 2012, según su artículo 15, si el reclamo presenta fallas, dentro de los cinco (5) días hábiles siguientes a la recepción de la solicitud, deberá informarse al solicitante para que subsane las fallas, para lo cual tendrá dos (2) meses para hacerlo, si no lo hace en este tiempo, se entenderá que desistió del reclamo; si quien recibe el reclamo no es competente para atenderlo, tendrá dos (2) días hábiles para darlo a conocer al solicitante. Sobre los datos que sean objeto de procesos judiciales, deben identificarse como “reclamo en trámite” (Ley 1581, artículo 18, literal h).

9. El Decreto 1727 de 2009, establece los requisitos mínimos que deben integrar los operadores de la información al momento de presentar información del titular, por lo que da los lineamientos que se deben tener en cuenta para adoptar un formato que cumpla con los requisitos de ley, y que atienda a las necesidades contractuales dependiendo de su naturaleza. Estos formatos deberían incluir la siguiente información, dependiendo del sector:

- Los siguientes datos siempre deben ser diligenciados en el formato, sin embargo, en cada reporte de información debe añadirse un encabezado que diga “Se presenta reporte negativo cuando la(s) persona(s) naturales y jurídicas efectivamente se encuentran en mora en sus cuotas u obligaciones. Se presenta reporte positivo cuando la(s) persona(s)

naturales y jurídicas están al día en sus obligaciones"[41]. Esto implica que se siga el siguiente formato.

Tabla 1. Formato para presentación de información del titular por parte del operador de la información.

Nombres y apellidos completos / Razón o denominación social (bien sea persona natural o jurídica):	
Tipo y número de identificación:	
Fecha de corte de la información (que se está reportando):	
Registro últimas consultas (número de consultas realizados en los últimos 6 meses):	
Fecha de la consulta (en la que se hace consulta de la información):	

- Los siguientes datos se deben incluir para las compañías financieras, vigiladas por la Superintendencia Financiera de Colombia, y las que se refiere el artículo 39 de la Ley 454 de 1998.[42]

Tabla 2. Formato para datos que deben incluir las compañías financieras para la presentación de información.

[41] PRESIDENCIA DE LA REPÚBLICA. Decreto 1727 del 15 de mayo de 2009. Art. 1.
[42] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 454 de 1998. Art. 39.

Tipo de contrato (celebrado entre el titular y la fuente de la información):	
Número y estado del contrato (se deben ocultar algunos números para efectos de seguridad y especificar si se encuentra vigente o no):	
Condición o calidad (en la que actúa el titular):	
Fuente de información (nombre de la persona natural o jurídica):	
Cupos aprobados (total):	
Cupo utilizado:	
Saldo a la fecha de corte:	
Número de cuotas pactadas:	
Número de cuotas pagadas:	
Estado de la obligación (al día o en mora):	
Situación o estado del titular (concordato, liquidación forzosa, liquidación voluntaria, proceso de reorganización u otra, o ninguna y debe indicarse expresamente):	
Pago de la obligación (si fue de forma voluntaria o no):	
Fecha de pago o extinción de la obligación (en la que se pagó o extinguió):	
Reestructuración:	
Reclamo o discusión judicial (si existe):	

- La siguiente información se solicitará en los casos en los que no se refieran a los casos anteriores:

Tabla 3. Formato para casos en que no apliquen los anteriores casos.

Tipo de contrato (celebrado entre el titular y la fuente de la información):	
Número del contrato (se deben ocultar algunos números para efectos de seguridad):	
Condición o calidad (en la que actúa el titular):	
Fuente de información (nombre de la persona natural o jurídica):	
Fecha de inicio de la obligación o activación del producto o servicio adquirido:	
Término o vigencia del contrato (especificar también el tiempo que lleva ejecutándose):	
Valor del cargo fijo:	
Cupo de crédito (cupo utilizado):	
Cláusula de permanencia:	
Saldo a la fecha de corte:	
Valor de la cuota:	
Número de cuotas pactadas:	
Número de cuotas pagadas:	
Estado de la obligación (al día o en mora):	
Saldo en mora (al momento de corte):	
Pago de la obligación (si fue de forma voluntaria o no):	
Fecha de pago o extinción de la obligación (en la que se pagó o extinguió):	
Refinanciación:	
Reclamo o discusión judicial (si existe):	

10. Los datos sensibles, de acuerdo al artículo 6 de la Ley 1581 de 2012, sólo podrán ser tratados si el titular da su expresa autorización, cuando sea necesario para salvaguardar los intereses vitales del titular, cuando se efectúe de forma legítima y con las debidas garantías para su protección y cuya finalidad sea política, filosófica, religiosa o sindical; cuando sea necesario conocerse para la defensa de algún derecho en el ámbito judicial, o cuando tenga una finalidad histórica, estadística o científica, caso en el cual, se debe ocultar la identidad del titular.

11. En el caso de solicitarse información, se podrá proporcionar por cualquier medio, ya sea físico o electrónico, depende de cómo lo requiera el titular de los datos, debe ser sencillo de leer, sin impedimentos para acceder a ella, y respetando el principio de transparencia (Ley 1581 de 2012, artículo 11), y sólo podrá suministrarse a los titulares, causahabientes o representantes legales, entidades públicas o administrativas en ejercicio de sus funciones, y los terceros debidamente autorizados por el titular o por la ley (Ley 1581 de 2012, artículo 13).

12. Se debe informar a la autoridad de protección de datos los casos en los que se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información. (Ley 1581 de 2012, artículo 17, literal n, artículo 18, literal k). No se puede circular la información que sea objeto de controversia y que la Superintendencia de Industria y Comercio haya ordenado su bloqueo (Ley 1581 de 2012, artículo 18, literal i).

13. No se permitirá la transferencia de datos a países que no demuestren contar con los niveles adecuados de protección de datos, salvo en los casos en los que el titular expresamente lo autorice, cuando se realice por razones de salud o higiene pública, cuando se trate de transferencias bancarias o bursátiles, cuando haya acordado la transferencia en virtud de los tratados internacionales suscritos por Colombia, para la ejecución contractual o en la etapa precontractual, y en los casos legalmente exigidos para salvaguardar el interés público, o para el reconocimiento o defensa de un derecho en instancias judiciales. (Ley 1581 de 2012, artículo 26).

14. Retomando nuevamente el tema de la autorización, se deben tener en cuenta varios aspectos, además de los ya revisados anteriormente:

- Sólo se deben recolectar los datos que sirvan para la consecución de la finalidad con la que se recolectan, atendiendo a los principios de finalidad y libertad. Por órdenes de la Superintendencia de Industria y Comercio, se debe proveer una descripción de los procedimientos que se usan para

la recolección, almacenamiento, uso, circulación, supresión de información, las finalidades y la necesidad de la recolección de los datos en cada caso. No deben utilizarse medios engañosos o fraudulentos para la recolección y tratamiento de los datos (Decreto 1377 de 2013, artículo 4).

- El único momento que se tiene para obtener la autorización es cuando se efectúa la recolección. En caso de que, el Responsable del Tratamiento modifique las políticas, en lo que se refiere a la identificación del Responsable del Tratamiento y la finalidad del tratamiento de los datos, se deberá informar al Titular, antes de implementarlas o al momento de hacerlo, y deberá obtener autorización del Titular para las finalidades que se estén introduciendo a la Política (Decreto 1377 de 2013, artículo 5). Esto entonces significa que la inclusión de nuevas finalidades debe ser analizado profundamente con el fin de evitar que un cambio en las políticas pueda representar para el Responsable de la información una situación de riesgo frente al uso indebido de la información.
- Respecto de los datos sensibles, se debe informar al Titular que, por tratarse de datos sensibles, no está obligado a dar su autorización, indicarle cuáles de los datos que se recolectarán son sensibles, cuál es su finalidad y obtener su consentimiento expreso. Ningún titular está obligado a otorgar datos sensibles, salvo los casos expuestos por la Ley 1581 de 2012. (Decreto 1377 de 2013, artículo 6).
- Se debe garantizar la consulta de la autorización otorgada por el Titular. La autorización se podrá otorgar mediante mecanismos predeterminados para que el Titular manifieste su autorización de manera automatizada. Se entiende válida la autorización cuando sea otorgada de forma escrita, oral o mediante conductas que permitan concluir de forma inequívoca y razonable tal autorización. El silencio no puede asimilarse como conducta inequívoca (Decreto 1377 de 2013, artículo 7).
- El Titular tiene en todo momento el derecho de solicitar al Encargado o al Responsable, la revocatoria de la autorización y/o la supresión del dato mediante la presentación de un Reclamo, en los términos anteriormente

mencionados; esto no procederá en los casos en los que por Ley o contrato deba permanecer la información en las bases de datos. Se deben permitir mecanismos de fácil acceso a los Titulares para presentar sus solicitudes. (Decreto 1377 de 2013, artículo 9).

- Se deben documentar los procedimientos que se utilizan para el tratamiento, conservación y supresión de los datos personales. (Decreto 1377 de 2013, artículo 11).

Recomendación: Sería pertinente dejar expreso en el contrato, que el PROVEEDOR sólo tratará los datos para los fines para los cuales fueron recolectados, y para lo cual el titular, dio su titular; si, llegado el caso, el PROVEEDOR efectuare un tratamiento, para un fin que no autorizó el titular, por directriz del CLIENTE, y por esta razón surge un reclamo, se debe eximir al PROVEEDOR de toda responsabilidad. Es por esto, que se debe contar con soporte de los procesos que se establecen para el tratamiento de los datos, junto con las directrices que dicte el CLIENTE para la ejecución del contrato de prestación de servicios suscrito con el PROVEEDOR.

15. Respecto de la Política y el Aviso de Privacidad, se debe conservar el modelo que se utiliza para dar a conocer la existencia de la Política de Tratamiento de Datos, ya sea por medios informáticos, electrónicos o cualquier otro mecanismo tecnológico que cumpla con lo dispuesto en la Ley 527 de 1999. Para la difusión de la política, tanto el CLIENTE como el PROVEEDOR, se podrán valer de medios físicos, documentales, como electrónicos, verbales o cualquier otro mecanismo que garantice el cumplimiento del deber de informar al Titular. (Decreto 1377 de 2013, artículos 16 y 17).

Es, por lo tanto, necesario establecer mecanismos permanentes de manera que los Titulares puedan acceder a sus datos personales y ejercer sus derechos sobre ellos, se les debe permitir su consulta por lo menos una vez al mes de forma gratuita y cada vez que se modifiquen de manera sustancial las políticas de tratamiento.

16. En la Compañía, se debe tener a una persona o área encargada de la protección de los datos personales, que permita darle trámite a las solicitudes de los titulares, sin embargo, se recomienda, que sean los CLIENTES quienes conserven la obligación de atender estos trámites, y por tanto, el PROVEEDOR, deberá atender los términos de ley (o los establecidos contractualmente) para hacer traslado de las solicitudes. (Decreto 1377 de 2013, artículo 23). Los operadores o encargados, además, deben proporcionar los medios idóneos para la recepción de consultas, peticiones y reclamos, como las líneas telefónicas o medios virtuales para el efecto. Circular Única Superintendencia de Industria y Comercio, Título V, numeral 1.7).

17. Todas las medidas que se relacionan en la presente guía, deben ser demostrables, es decir, no basta sólo con redactar las políticas de tratamiento o los avisos de privacidad, ni con los contratos de transmisión de datos; sino que, hay que demostrar que se está en capacidad de cumplir con los requisitos establecidos por Ley, y que las medidas que han implementado son efectivas; además, se deben identificar los riesgos potenciales que se puedan causar a los titulares como consecuencia del tratamiento. (Decreto 1377 de 2013, artículo 26).

Se debe garantizar, que la Compañía posee una estructura administrativa que atiende la estructura y tamaño de la empresa para que las medidas estén ajustadas a la Ley; que adopta los mecanismos suficientes para implementar las políticas, lo que incluye también entrenamiento y programas de educación; y que tiene procesos organizados para la atención de consultas, peticiones y reclamos (Decreto 1377 de 2013, artículo 27).

18. Para efectuar la entrega de la información confidencial y atender las consultas, peticiones y quejas, se deben tomar medidas de seguridad, las cuales requieren que se verifique la calidad del titular, si es de forma personal, se debe mostrar el documento idóneo para el efecto, y si es de forma telefónica, si el PROVEEDOR tiene la opción, debe validarse la información pertinente que

permita su identificación, y debe quedar un registro de su llamada. Si la solicitud se efectúa mediante apoderado o persona autorizada, se debe presentar el respectivo poder otorgado por el Titular. Si la petición la realizan los causahabientes del Titular, se debe verificar la calidad de quien formula la consulta o petición. Si son personas jurídicas quienes presentan la petición, se deberá proporcionar la identificación del representante legal junto el documento que acredite la existencia y representación de la persona jurídica, esto no será necesario si ya cuentan con esa información o si está contenida en bases de datos públicas. Si son entidades públicas quienes solicitan la información, se debe verificar que tal solicitud tiene una finalidad concreta para la cual solicitan la información y cuáles son sus funciones conferidas por ley para tal finalidad (Circular Única de la Superintendencia de Industria y Comercio, Título 5, numeral 1.1).

La respuesta a las peticiones efectuadas de manera verbal, o por medios electrónicos, deberán contar con la prueba de dicha respuesta, conservando copia de la respuesta, o la grabación de la misma. (Circular Única Superintendencia de Industria y Comercio, Título V, numeral 1.7).

19. Hay que tener en cuenta que, a la Superintendencia de Industria y Comercio, los operadores deben remitir una copia de las Políticas de Tratamiento de Datos Personales, a la Delegatura para la Protección de Datos Personales, y cada vez que se haga una modificación a tales Políticas, también se debe enviar una copia. La Superintendencia podrá formular observaciones y solicitar correcciones, las cuales se deben resolver en el tiempo en que ella lo establezca.

Dentro de los primeros diez (10) días hábiles de los meses de febrero y agosto, el Encargado debe enviar a la Delegatura, una constancia, suscrita por el Representante Legal, en la que se dé cuenta que se solicitó, semestralmente, la certificación de la autorización al Responsable, con corte al 31 de diciembre y 30 de junio. Y, en los meses de marzo y septiembre, los primeros diez (10) días, se deberá informar a la Superintendencia, cuáles fueron esos Responsables que no

cumplieron con el deber de la certificación, indicando su nombre o razón social, su identificación, la última dirección registrada, la fecha en la cual se solicitó la certificación. Si el Responsable no envía la certificación en los términos anteriormente mencionados, el Encargado deberá bloquear la información, máximo por veinte (20) días, hasta que el Responsable proporcione el certificado (Circular Única de la Superintendencia de Industria y Comercio, Título V, numeral 1.2).

Por otro lado, los Encargados u Operadores, deberán también presentar un informe a la Superintendencia, los primeros quince (15) días hábiles de febrero y agosto de cada año, en un archivo en Excel, editable, que contenga la siguiente información:

- Número de reclamos hechos a los operadores o encargados por los titulares.
- Especificar nombre e identificación de la fuente o responsable.
- Identificar causa del reclamo.
    - Si es causado por la información reportada por la Fuente o el Responsable, se debe informar la cantidad de titulares reportados por él.

20. De acuerdo con la Circular Única, de la SIC, Título 5, numeral 1.9, los reclamos que hagan los titulares de la información deben seguir una tipología, que se presenta a continuación:

Tabla 4. Tipologías y subtipologías de reclamos por parte de titulares sobre uso de información[43].

[43] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Circular única. Título V: Protección de datos personales. Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/Titulo%20V%20Proteccion_Datos_Personales.pdf

TIPOLOGÍA DE RECLAMOS	SUBTIPOLOGÍA DE RECLAMOS	CÓDIGO NUMÉRICO
Actualizar información	No actualización de la información	01
	No reporte de información oportuno	02
	Reporte de información incompleta o parcial	03
	No inclusión de las respectivas leyendas	04
	Inconformidad con la permanencia de la información negativa	05
Rectificar la información	No rectificación de información errónea	06
	Inexistencia de la obligación reportada o negación de la relación contractual	07
	No contar con los documentos soporte de la obligación	08
	No contar con la autorización previa y expresa del titular para reportar información	09
	No certificar semestralmente al operador que la información suministrada cuenta con la respectiva autorización del titular	10
	No remitir la comunicación previa al reporte	11
Conocer la información	Negación de acceso a la información	12
	No atender las peticiones y reclamos presentados por los titulares de fondo y oportunamente	13
	No adoptar las medidas de seguridad adecuadas sobre la información obtenida en las bases de datos de los operadores	14
	Utilizar la información para una finalidad diferente a aquella para la cual fue entregada	15
	Consulta de información no autorizada por el titular, cuando esta sea requerida	16
	No contar con medidas adecuadas de seguridad	17
	No informar al titular sobre la utilización que se le está dando a su información	18
	No informar al titular la finalidad de la recolección de la información	19
	No guardar reserva sobre la información obtenida en las bases de datos de los operadores	20
	Otros (Describir el motivo)	21

21. Respecto del Registro Nacional de Base de Datos (en adelante, RNBD), se debe tener en cuenta lo siguiente:

- Lo deben implementar las compañías Responsables sobre tratamiento de datos personales, así como sociedades y entidades sin ánimo de lucro, cuyos activos totales sean iguales o superiores a los 100.000 UVT (Unidades de Valor Tributario), que para el año 2022, equivalen a $3.800.400.000; deberán realizar la respectiva inscripción y seguir lo establecido en el Manual de Usuario del Registro Nacional de Bases de Datos.

- Siempre que surjan cambios en la información suministrada, dentro de los diez (10) días hábiles siguientes a la modificación, deberá actualizarse en la plataforma destinada para el RNBD, al igual que debe actualizarse cada año, el día 2 de enero y el 31 de marzo. Los cambios que deben ser actualizados son aquellos que tengan que ver con la persona o entidad que ostenta la calidad de encargado, los canales de atención, la clasificación o tipo de datos personales almacenados, las medidas de seguridad, la Política de Tratamiento de la información, la transferencia y transmisión internacional de los datos. (Circular Única, Título V, Numeral 2.3).
- Los Responsables del Tratamiento que no estén inscritos en cámaras de comercio, deberán registrar la siguiente información en el RNBD (Circular Única, Título V, Numeral 2.5):
    - Clasificación de la información almacenada en las bases de datos.
    - Medidas de seguridad de la información.
    - Procedencia de los datos personales.
    - Identificación del destinatario en caso de transferencia internacional de bases de datos, su ubicación, y si cumple con lo determinado por la Delegatura para la Protección de Datos, y lo contenido en el artículo 26 de la Ley 1581 de 2012.
    - Identificación del destinatario en caso de transmisión internacional de bases de datos, su ubicación, y determinar si tienen un contrato de transmisión suscrito en los términos del Decreto 1074 de 2015, artículo 2.2.2.25.5.2.
    - La identificación del cesionario en caso de cesión o transferencia nacional de bases de datos. La cesión no se debe registrar, pero el cesionario debe cumplir con el registro de la base de datos cedida.
    - Reportar como novedades los reclamos o incidentes de seguridad.
- La información que debe contener el RNBD, es el siguiente:[44]

[44] PRESIDENCIA DE LA REPÚBLICA. Decreto 886 de 2014, Art. 5.

- Datos de identificación del Responsable (Razón social y NIT si es persona jurídica, documento de identidad si es persona natural), su ubicación y contacto.
- Datos de identificación del Encargado (Razón social y NIT si es persona jurídica, documento de identidad si es persona natural), su ubicación y contacto.
- Canales para el ejercicio de los derechos de los titulares. (Se debe garantizar que por lo menos, el canal por medio del cual se recogió la información del Titular, sea el canal por donde el Titular pueda ejercer sus derechos.)
- Nombre y finalidad de los datos.
- Forma de tratamiento de los datos (automatizada y/o manual).
- Política de tratamiento de la información.
- Además de la información que la SIC pueda requerir en ejercicio de sus funciones.

22. Al respecto de la duración de la conservación de los datos personales, sólo se podrán recolectar, usar, almacenar o circular, durante el tiempo que sea razonablemente necesario en atención a la finalidad con la cual fue recolectada la información, atendiendo además a aspectos administrativos, contables, fiscales, jurídicos e históricos. Una vez cumplida la finalidad, y sin perjuicio de lo dispuesto por la ley, se deberán suprimir o eliminar los datos, salvo expreso mandato legal o contractual.[45]

23. Respecto de la transferencia y transmisión internacional de los datos personales, no se deberá informar al Titular, si el Responsable y el Encargado efectúan dicha operación con el fin de que el Encargado realice el tratamiento por cuenta del Responsabilidad, siempre que cumplan con la suscripción del contrato de transmisión de datos, el cual debe contener y cumplir como mínimo, tratar los datos a nombre del Responsable de acuerdo a los principios que los

[45] PRESIDENCIA DE LA REPÚBLICA. Decreto 1074 de 2015, Art. 2.2.2.25.2.8.

protegen, contar con mecanismos para salvaguardar la información y guardar estricta confidencialidad respecto del tratamiento.[46]

24. Se debe tener en cuenta que la Ley 1928 de 2018, reglamenta para Colombia el Convenio sobre la Ciberdelincuencia celebrado en Budapest, el pasado 23 de noviembre de 2001, celebrado entre los miembros del Consejo de Europa y los países que firmaron el acuerdo. Este convenio contiene la identificación de delitos en torno a la ciberdelincuencia, junto con aspectos que deben tener en cuenta cada ordenamiento jurídico, y entre ellos, surge la necesidad de que se pueda garantizar la conservación rápida de datos informáticos almacenados, especialmente de aquellos que sean susceptibles de pérdida o modificación.

2.3.2. Sanciones

En este apartado, no sólo se hablarán de las sanciones que se han impuesto, sino también, de las sanciones que, según la ley, podrían imponerse.

1. La Superintendencia de Industria y Comercio (en adelante SIC), sancionó a Casa Editorial El Tiempo S.A. con cincuenta (50) salarios mínimos legales mensuales vigentes puesto que un titular presentó una petición por medio de correo electrónico ejerciendo su derecho al *habeas data*, El Tiempo contaba con diez (10) días para atender la petición, sin embargo, se dio respuesta tres (3) meses después de realizada la petición; la Superintendencia adujo que El Tiempo no implementó las medidas necesarias para dar trámite, pese a la gran cantidad de datos personales que trata la entidad.[47]

2. La SIC sancionó a la Compañía Nacional de Chocolates S.A.S., con la suma de ciento cincuenta (150) salarios mínimos mensuales legales vigentes, por

---

[46] Ibid. Art. 2.2.2.25.5.1. y 2.2.2.25.5.2.
[47] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, Resolución 71307 del 28 de noviembre de 2014.

haber divulgado en internet, y sin las medidas de seguridad idóneas, la base de datos personales, en cuya página web, reposaba la información de 7.671 titulares más; violando así el artículo 4 de la Ley 1581 de 2012.[48]

3. En palabras de la SIC, la Ley 1581 de 2012 aplica a cualquier tratamiento de datos, indistintamente de la forma en la que sean recolectados (física o virtualmente), y del momento en el que se recolecten (presente o futura); también afirma que el número telefónico es un dato personal en el momento en el que puede asociarse a alguna persona en específico, o sea, se puede atribuir a una persona este dato. Un Responsable del tratamiento, no puede excusarse afirmando que no cuenta con la prueba de la autorización de datos personales porque se obtuvieron por medios electrónicos; considera la Superintendencia que hacer uso de marcadores predictivos implica la automatización del tratamiento de datos personales. Para hacer el uso de marcadores predictivos, y, a manera de ejemplo, devolver la llamada cuando se solicite vía telefónica por el menú de IVR o por WhatsApp, se requiere la autorización del titular para sus datos personales, como el número de teléfono para el efecto. Por no cumplir con lo anteriormente expuesto, la compañía MERVICOL S.A.S. fue sancionada con la suma de 348,8566855 Unidades de Valor Tributario (UVT).[49]

4. La EPS SANITAS S.A.S. fue sancionada por la SIC, porque modificó la información de la residencia de una persona, sin que el titular de la información lo hubiera solicitado, causando que perdiera procedimientos médicos porque fue trasladado a otra EPS, y la EPS SANITAS se demoró más de 10 meses en corregir los datos del titular, por lo que recibieron una multa de $894.365.280.[50]

5. La SIC sancionó a CONTACTO SOLUTIONS LTDA con una multa de $264.997.120, entre otras cosas, porque la empresa no contaba con las

---

[48] SIC, Resolución 8483 del 27 de febrero de 2015.
[49] SIC, Resolución 17629 del 29 de mayo de 2019. Resolución 38281 del 14 de julio de 2020.
[50] SIC, Resolución 64328 del 19 de noviembre de 2019 y Resolución 77049 del 30 de noviembre de 2020.

autorizaciones de los titulares y no implementaba lo que determina la ley al respecto.[51]

6. La SIC tiene la facultad sancionar a aquellas compañías, que nieguen una solicitud de crédito, basados únicamente en su reporte negativo. (Ley 1266 de 2008, artículo 10).

7. La Ley 1273 de 2009 introduce un nuevo bien jurídico tutelado al Código Penal, el cual es la protección de la información y de los datos, en la que se establecen penas que van desde los treinta y seis (36) a los noventa y seis (96) meses de prisión, dependiendo del supuesto penal, y multas de cien (100) a mil (1.000) salarios mínimos legales mensuales vigentes, para los casos de acceso abusivo a sistema informático, pero también se incluye la interceptación de datos informáticos, el uso de software malicioso, la violación de datos personales, o la suplantación de sitios web para capturar datos personales (phishing), entre otros.

8. La sociedad REDCORD DE COLOMBIA S.A. BANCO NACIONAL DE CÉLULAS MADRE, recolectó y usó los datos de una mujer que se encontraba en gestación, con el fin de ofrecer sus servicios para la conservación de células madre del cordón umbilical; por esta razón la SIC sancionó a tal sociedad por el indebido tratamiento de datos sensibles, y porque además, la sociedad no pudo probar que contaba con la autorización expresa de la titular para el tratamiento de sus datos sensibles, como lo es su estado de salud, por lo que fue multada la sociedad por $123.200.000.[52]

9. La SIC podrá imponer multas de carácter personal o institucional hasta por dos mil SMMLV, y podrán ser sucesivas mientras subsistan las circunstancias que originaron la sanción; además, podrá ordenar la suspensión de actividades relativas al tratamiento de datos hasta por seis (6) meses, también podrá ordenar

---

[51] SIC, Resolución 6074 del 18 de marzo de 2019.
[52] SIC. Resolución 58969 de 29 de septiembre de 2014.

el cierre temporal de las actividades tendientes al tratamiento de datos si en el término de suspensión no se tomaron las medidas para corregir la infracción y finalmente, podrá ordenar el cierre definitivo de las operaciones que involucren tales actividades. Sobre las actuaciones cometidas por una entidad pública, conocerá la Procuraduría General de la Nación. (Ley 1581 de 2012, artículo 23).

10. La compañía MADEFORMAS S.A.S. fue sancionada por la SIC, mediante Resolución número 59472 el pasado 25 de septiembre de 2020, por incumplir con las instrucciones y requerimientos de la SIC, puesto que, aunque MADEFORMAS haya cumplido de forma extemporánea con la actualización de la información en el RNBD, no atendieron a lo requerido por la SIC al solicitarles que se desbloqueen los documentos que se habían cargado respecto de la Política de Tratamiento de Datos Personales de la Compañía, por esta razón fueron multados con la suma de $1.744.743.

2.4. NORMATIVIDAD APLICABLE A LA PROTECCIÓN DE DATOS PERSONALES EN LA UNIÓN EUROPEA

Como se ha mencionado, los negocios que tienen que ver con el Contact Center y BPO, se han convertido en un tipo de negocio que no conoce fronteras, lo que ha permitido que a Colombia, lleguen clientes que contraten este servicio provenientes de otros países, entre ellos, los que pertenecen a la Unión Europea; mantener buenas relaciones con tales clientes y dar cabal cumplimiento al contrato, implica además que los contratistas colombianos se encuentren en la capacidad de responder a los estándares que imponen estos clientes, y entre ellos están los estándares que versan sobre la protección de datos personales, y la Unión Europea, es uno de los organismos internacionales más exigentes en lo que a ello respecta. Cabe mencionar que, para la Unión Europea, la protección de datos personales no es en sí un derecho absoluto, sino que debe considerarse en conexidad con otros derechos fundamentales, tales como:

> *"el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística."*[53]

Es por lo anterior que se realizará una recopilación de las principales obligaciones que contiene el Reglamento General de Protección de Datos (por sus siglas en español, y en adelante, "RGPD"), expedido el 27 de abril de 2016, junto con las sanciones que su incumplimiento pueda traer.

2.4.1. Obligaciones desde el RGDP

1. Se permite el uso de herramientas tecnológicas y de la automatización para el tratamiento de los datos personales, sin embargo, no debe depender solamente de estas técnicas, sino que también, debe darse un tratamiento manual, con el fin de no eludir la responsabilidad.[54] Esa automatización, o la que incluya la elaboración de perfiles, debe contar con métodos matemáticos o estadísticos para que se puedan aplicar las medidas técnicas, al igual que las medidas organizativas respectivas, y así, corregir los factores que ocasionan inexactitudes, y reducir el riesgo al error, para que se protejan los derechos y los intereses de los titulares o interesados.[55]

2. El reglamento da a entender que las actividades en redes sociales, o en línea, son consideradas actividades personales o domésticas, y deberá cumplirse con el tratamiento de datos cuando, en ejercicio de actividades comerciales o profesionales, los responsables o encargados corran por su cuenta con poner a

---

[53] OP. Cit. RGDP. Pag. 2.
[54] Ibid. Pág. 3. Núm 15.
[55] Ibid. Pág. 4. Núm. 71.

disposición los medios para tratar datos personales relacionados con esas actividades personales y domésticas.[56] Los datos recolectados para fines científicos, históricos, y estadísticos, deben recolectarse y tratarse atendiendo al principio de minimización de los datos, es decir, usar única y estrictamente los datos necesarios, que pueda ser posible no identificar al titular de la información, y también, se deben atender a los principios de proporcionalidad y de necesidad.[57] Esa minimización, implica la pseudonimización de los datos, de forma tal que, si en un futuro llegan a tratarse los datos para los fines mencionados al inicio del párrafo, no debe ser posible de ninguna forma, identificar a quién pertenecían tales datos.[58]

3. De acuerdo con el Reglamento, los responsables o encargados ubicados en terceros países, diferentes a los de la Unión Europea, deben cumplir con el RGPD, cuando se trate de personas que residan en algún país miembro de la Unión, y cuando se traten los datos de tales personas con el fin de ofrecer bienes y servicios, sin que necesariamente, haya un pago de por medio; siempre que se logre demostrar, que ese responsable o encargado está proyectándose a ofrecer bienes y servicios a personas que residan en países de la Unión, bien sea por lenguaje, la posibilidad de adquirir esos bienes y servicios por cualquier persona en la Unión Europea, o porque la moneda con la que se ofrezcan esos servicios sea la utilizada normalmente en uno o varios países miembros de la Unión.[59]

Recomendación: Esto podría implicar que, si alguna persona que resida en algún país de la Unión Europea, se comunica con un Contact Center en Colombia, bien sea porque está de viaje en Colombia por vacaciones o negocios, y esa persona pretende adquirir algún bien o servicio, los datos de esa persona deben tratarse de acuerdo al RGPD.

---

[56]Ibid. Pág. 4. Núm. 18.
[57] Ibid. Pág. 29. Núm. 156.
[58] Ibid. Art. 89. Núm 1.
[59] Ibid. Pág. 5, Núm 23.

4. Si por ejemplo, un país externo a la Unión Europea, realiza el tratamiento de los datos personales asociados al comportamiento de personas físicas ubicadas en la Unión, como efectuar un perfilamiento de una persona respecto de sus preferencias, comportamientos o actitudes, y hacerles un análisis, también debe cumplirse con el Reglamento.[60] También se menciona que, en caso de darse un tratamiento a los datos, diferente del autorizado, es permitido si tiene que ver con las actividades lícitas de acuerdo al reglamento, entre ellas, cuando se traten los datos para fines científicos, históricos o estadísticos, sin que haya necesidad de una nueva autorización para ello[61], sin embargo, se debe informar al interesado, y se debe garantizar en todo momento el derecho de oposición. El Responsable del tratamiento en estos casos, debe destinar a un representante para que pueda ser contactado en cualquier momento por un organismo de control, a este representante o encargado, se le deberá otorgar la facultad para actuar en su nombre para el tratamiento de los datos por medio escrito y se le debe someter a medidas coercitivas en caso de que incumpla con lo estipulado para el tratamiento de datos personales, adicional a ello, se debe limitar la recolección de datos a lo estrictamente necesario para los fines para los que se recolectan, y omitir o evitar recolectar información respecto de la situación jurídica de la persona, de las sanciones y penas que esta pueda tener a su nombre.[62]

Recomendación: Eso quiere decir, que, en caso de que se encargue a una compañía en Colombia, la actividad de análisis y perfilamiento (que es práctica usual en los Contact Center, con el fin de mejorar la prestación de sus servicios), a personas residentes en la Unión Europea, debe cumplirse con el Reglamento, lo que permite inducir que la tecnología no puede subsistir por sí sola, pues es necesario conocer los límites que le impone la ley para su correcto uso.

---

[60] Ibid. Pág. 5. Núm 24..
[61] Ibid. Pág. 9, Núm. 50.
[62] Ibid. Pág 15, Núm 80.

5. Con el fin de evitar que los datos sean recolectados o almacenados por más tiempo del estrictamente necesario, el Responsable debe establecer plazos fijos para que se efectúe la supresión o la revisión periódica, debe garantizarse esa rectificación y la supresión de datos inexactos.[63]

6. En lo que se refiere a la autorización del tratamiento, el Reglamento sugiere, que se viola al titular de dar su libre consentimiento para el tratamiento, cuando no se permite autorizar de manera separada cada una de las finalidades del tratamiento, o de las actividades que se llevarán a cabo.[64]

7. El Responsable debe poner a disposición del titular de los datos, medios electrónicos para presentar sus solicitudes respecto de sus datos, adicional a ello, el plazo para dar respuesta al titular es máximo de un mes, y en caso de no atender la solicitud, se deberán explicar los motivos.[65]

8. El Reglamento menciona que en los casos en los que hayan formatos electrónicos, los íconos deben poder ser legibles de forma mecánica.[66]

9. Los riesgos que prevé el Reglamento y que pueden tener una ocurrencia viable se refieren al tratamiento de datos que puedan ocasionar daños físicos, materiales o inmateriales, que puedan ocasionar discriminación, robo de identidad o fraude, pérdidas financieras, daño a la reputación, revelación de información confidencial o secreto profesional, pero también la pérdida, destrucción, alteración ilícita o accidental, y la divulgación no autorizada; a la imposibilidad que tengan los titulares de ejercer sus derechos y de tener el control sobre sus datos; a la revelación de datos sensibles, incluidas las condenas o infracciones penales; al tratamiento de datos de personas consideras vulnerables como los niños; y a los escenarios en los que implican el

---

[63] Ibid. Pág. 7. Num. 39.
[64] Ibid. Pág. 8. Núm. 43.
[65] Ibid. Pág. 11. Núm. 59.
[66] Ibid. Pág. 12. Núm. 60.

tratamiento de una gran cantidad de datos personales y muchos de los titulares puedan llegar a verse afectados.[67]

Se deben identificar los riesgos que puedan ocurrir respecto del tratamiento de los datos, se debe evidenciar además la probabilidad de ocurrencia y la gravedad, antes de efectuarse el tratamiento[68], también se deben identificar las medidas suficientes para mitigar los riesgos, los mecanismos para garantizar la protección, y demostrar que las tales son de acuerdo con el Reglamento.[69] El Encargado debe apoyar al Responsable, en los casos en los que se solicite o cuando sea necesario, para la evaluación de riesgos o de impacto.[70]

El Reglamento estipula que la autoridad de control publicará una lista de aquellos datos personales a los que se les deberá aplicar una evaluación de impacto previo al tratamiento, tales listas serán comunicadas al Comité[71]; al igual que las listas de los datos que no requieren evaluación de impacto.[72] Las evaluaciones de impacto deberán contener por lo menos descripción de las operaciones para efectuar el tratamiento, los fines, y según sea el caso, el interés legítimo que busca el Responsable; establecer la relación entre la proporcionalidad y necesidad de las operaciones y los fines anteriormente descritos y finalmente, enumerar las medidas que se tienen previstas para mitigar los riesgos, garantizar la seguridad y demostrar el cumplimiento del Reglamento.[73]

Recomendación: Aunque la evaluación de impacto esté limitado a la lista comunicada por el Comité de la Unión Europea, se puede considerar una buena práctica empresarial, realizar las evaluaciones de impacto en la etapa de

---

[67] Ibid. Pág. 15. Núm. 75.
[68] Ibid.
[69] Ibid. Pág. 17. Núm 90.
[70] Ibid. Pág. 18. Núm 95.
[71] Ibid. Art. 35. Núm 4..
[72] Ibid. Art. 35. Núm 5..
[73] Ibid. Núm 7..

implementación para dar comienzo a la ejecución de contratos que requiera el tratamiento de datos, bien sean nacionales o provenientes de la UE.

10. El Reglamento exige que las medidas que se implementen para cumplirlo, deben ser comprobables, entre las medidas que sugieren están *"reducir al máximo el tratamiento de datos personales, pseudonimizar lo antes posible los datos personales",* cumplir los principios para el tratamiento de datos, y optimizar la seguridad. De igual forma, en los casos en los que se llegue a solicitar por encargo algún producto, servicio o aplicación, debe solicitarse y asegurarse igualmente que se cumplan con el reglamento de protección de datos.[74] Entre las medidas que se pueden imponer a los encargados del tratamiento están por un lado, que se adhieran a un código de conducta, y por el otro lado, que por medio de alguna certificación se compruebe el cumplimiento, además de que debe mediar un contrato u otro documento jurídico idóneo, el cual debe contener por lo menos, objeto, duración del tratamiento, la naturaleza, los fines del tratamiento, el tipo de datos que se tratarán, la categoría de los interesados, establecer las funciones y responsabilidades, y prever el riesgo para los interesados. [75] Una vez hecho esto, si se encuentra que las medidas contempladas no son suficientes para mitigar los riesgos e implicaría la potencial violación de derechos y libertados de los titulares, antes de efectuar el tratamiento, se debe consultar con la autoridad competente.

Otras de las medidas de seguridad que sugiere el Reglamento son cifrar los datos, garantizar la resiliencia permanente de los sistemas y servicios de tratamiento (además de la confidencialidad, integridad y disponibilidad), restaurar la disponibilidad y acceso de los datos en caso de incidentes rápidamente, y contar con procesos de verificación, evaluación y valoración de la eficacia de las medidas para garantizar la seguridad de forma periódica.[76]

---

[74] Ibid. Pág. 15. Núm. 78.
[75] Ibid. Pág. 16. Núm. 81.
[76] Ibid. Art. 32.

11. En el caso en que suceda un hecho, que implique la violación de la seguridad de los datos personales, se tendrán máximo 72 horas, después de haberse conocido la ocurrencia del hecho, para reportarlo a la autoridad de control competente. Si llegado el caso, no pudiera hacerse tal reporte dentro de las 72 horas, se deberá realizar explicando cuáles fueron las razones para la demora. Tal reporte no es estrictamente imperioso hacerlo, en los casos en los que se pueda demostrar que tal violación, no implica necesariamente un riesgo a los derechos y libertades de las personas físicas.[77] De igual manera, se debe notificar al interesado con prontitud sobre la ocurrencia del hecho, especificando cuál es la naturaleza de la violación, y las recomendaciones para que el interesado pueda de alguna manera, mitigar los efectos de la violación de la seguridad.[78] Si bien esta obligación está orientada al Responsable del tratamiento, es recomendable que el PROVEEDOR de una empresa europea, haga el respectivo reporte al Responsable de los datos de manera oportuna, en este caso el CLIENTE, para que este, haga el reporte ante la autoridad competente de su domicilio. De igual forma, si el hecho es advertido por el CLIENTE, este debería dar aviso oportuno al Encargado, para que éste, pueda adelantar todas las acciones necesarias para mitigar el riesgo.

El reporte debe, por lo menos, describir la naturaleza de la violación, si es posible, la categoría y cantidad de interesados y datos afectados; proporcionar el nombre y el contacto del delegado de protección de datos o de la persona disponible que pueda dar información; especificar las posibles consecuencias; establecer cuáles fueron las medidas que se tomaron o propusieron y qué medidas se implementaron para mitigar efectos adversos. Si la información no puede proporcionarse de forma sincrónica, se podrá realizar de forma escalonada sin demorarse más de lo debido.[79]

---

[77] Ibid. Pág. 16. Núm. 85.
[78] Ibid. Pág. 17. Núm. 86.
[79] Ibid. Art. 33. Núm 3 y 4.

12. Se deben elaborar códigos de conducta, que permitan aplicar el Reglamento de manera efectiva, que contenga las obligaciones que debe cumplir el Encargado, teniendo en cuenta los riesgos que implica el tratamiento de los datos, para que los delegados puedan cumplir a cabalidad con sus funciones.[80]

13. Para hacer transferencia de datos a países terceros, fuera de la Unión Europea, se debe garantizar y comprobar que el Encargado ubicado en un país tercero, tiene todas capacidades para cumplir con el Reglamento.[81] Además, el tercer país debe respetar el Estado de Derecho, garantizar el acceso a la justicia, cumplir las normas sobre derechos humanos, y garantizar acciones administrativas judiciales y efectivas para que los interesados puedan ejercer sus derechos respecto de sus datos.[82] Se prefiere que el país con el que se haga la transferencia de datos, haya suscrito el Convenio del Consejo de Europa, del 28 de enero de 1981,[83] (Colombia aún no se ha adherido al Convenio, en la página del Consejo de Europa, se menciona en una noticia del 30 de agosto de 2019, que Colombia podría participar en reuniones del Comité 108 en calidad de observador, antes de adherirse al Convenio[84]), en todo caso, se debe demostrar que se cuenta con garantías necesarias y adecuadas para proteger a los interesados, entre ellas, contar con normas corporativas vinculantes, incorporar las Cláusulas establecidos por el Consejo de Europa, que, recientemente, el 4 de junio de 2021, se actualizaron; o incorporar cláusulas admitidas por algún órgano de control.[85]

---

[80] Ibid. Pág. 19. Núm 98.
[81] Ibid. Pág. 19. Núm 101.
[82] Ibid. Pág. 20. Núm. 104.
[83] Ibid. Pág 21. Núm. 105.
[84] COUNCIL OF EUROPE. Colombia: Un primer paso hacia el Convenio. 30 de agosto de 2019. [Online] https://www.coe.int/es/web/data-protection/-/colombia-a-first-step-towards-convention-108-
[85] Op. Cit. RGPD. Pág. 20, Núm. 108.

En caso de que el Titular lo requiera, se deberá informar sobre las garantías que tenga el Interesado respecto del tratamiento de sus datos realizado en terceros países.[86]

Recomendación: Se debe revisar la Decisión de Ejecución de la Unión Europea, del pasado 4 de junio de 2021, para conocer las cláusulas tipo, y poderlas implementar en los contratos, no sólo con Clientes para los que se traten datos personales de personas residentes en países de la Unión Europea, sino también para reforzar las garantías que como proveedores colombianos se podrían otorgar sobre el tema.

14. Un principio importante que contiene el RGPD, es el principio de responsabilidad proactiva, que implica que el cumplimiento del reglamento, pueda ser demostrado; lo que supone que se debe contar con evidencias de todas las acciones que se adelanten para el tratamiento y la protección de los datos[87]; las cuales deben revisarse y actualizarse siempre que sea necesario[88] Uno de los mecanismos que prevé el Reglamento para demostrar su cumplimiento, es la expedición de certificaciones, conforme a lo que establece el artículo 42.

15. El Reglamento incluye una estipulación muy importante respecto del consentimiento del interesado para el tratamiento de los datos personales, estableciendo que, si la declaración contiene aspectos que de alguna manera viole lo consagrado en el Reglamento, no se entenderá vinculante.[89] El numeral 3 del artículo 7 menciona que *"Será tan fácil retirar su consentimiento como darlo"*, es un aspecto que debe garantizarse, por lo que deben establecerse todos los medios para que sea posible retirar el consentimiento con tal facilidad. Para que se dé la libertad en el otorgamiento del consentimiento, no podrá

[86] Ibid. Art. 15, Núm 2.
[87] Ibid. Art. 1. Núm. 2.
[88] Ibid. Art. 24. Núm. 1. .
[89] Ibid. Art. 7. Núm. 2.

someterse al interesado a que suministre datos que, para la prestación de un servicio o la ejecución de un contrato, no sean necesarios.[90]

16. Al tratarse de la transparencia de los datos, el Reglamento exige que las solicitudes que realice el interesado sobre las actuaciones del Responsable con respecto de sus datos, se debe dar respuesta dentro de un (1) mes contado a partir de recibida la solicitud, con una prórroga de dos (2) meses adicionales, indicando al interesado los motivos del retraso. Se debe presentar al interesado la respuesta por el medio que lo solicite, en caso de que lo especifique.[91] Adicional a ello, se debe dar una explicación al terminar el mes, del por qué no se dio respuesta en el tiempo indicado, y las posibilidades que tiene el interesado para presentar una reclamación y las autoridades ante quienes puede hacerlo.[92]

17. Sobre la temporalidad de los datos, el Reglamento adiciona que, en caso de que no se conozca en sí el tiempo determinado en el que se tratarán los datos, se deberá informar por lo menos la forma en la que podrá determinarse ese tiempo.[93]

18. Se debe garantizar que la supresión de los datos se realice sin dilación, aun así, se puede exceptuar la supresión de los datos en los casos en los que sean necesarios para ejercer el derecho de libertad de expresión e información, para atender una obligación impuesta por la Unión o sus estados miembros, por razones de salud pública, para fines históricos, científicos o estadísticos en el sentido en que torne imposible lograr el objetivo del tratamiento, y para efectos de reclamaciones.[94]

---

[90] Ibid. Art. 7. Núm. 4.
[91] Ibid. Art. 12. Núm. 3..
[92] Ibid. Art. 12. Núm. 4.
[93] Ibid. Art. 13. Núm. 3. Lit. e..
[94] Ibid. Art. 16. Núm. 3..

19. Si bien el ordenamiento colombiano establece que un Titular no puede verse afectado por una decisión que se tome basada en el tratamiento automatizado de los datos o en la elaboración de perfiles, el RGPD también lo consagra pero lo limita, pues no deberá aplicar cuando ese tratamiento sea necesario para que el Titular y el Responsable celebren o ejecuten algún contrato, cuando fue autorizado por la Unión o un Estado miembro, o cuando el tratamiento se basa en el consentimiento explícito otorgado por el titular.[95]

20. Para el tratamiento de los datos en países fuera de la Unión, el Responsable debe designar por escrito un representante en la Unión, en el Estado de residencia de las personas físicas titulares de los datos con el fin de que atienda a las consultas presentadas por las autoridades o los interesados.[96] Lo anterior, no será necesario si el tratamiento es ocasional, si no se tratarán datos a gran escala, o concernientes a condenas o infracciones penales y si no es probable la ocurrencia de algún riesgo.

21. El Encargado no puede ceder sus obligaciones a otro Encargado sin autorización del Responsable, quien tendrá derecho a oponerse. El tratamiento de los datos por medio del Encargado, se regirá por un contrato que lo vincule con el Responsable, y en el cual se debe establecer que, el Encargado tratará los datos de acuerdo con las instrucciones dadas por el Responsable de forma documentada (salvo previa exigencia legal aplicable al Encargado por parte de la Unión o un Estado miembro), así mismo, se deberá garantizar que las personas autorizadas a tratar los datos cumplan con el deber de confidencialidad y están sujetos a tal obligación. El Encargado deberá asistir al Responsable respecto de las solicitudes que presenten los interesados, garantizar la supresión de la información y sus copias una vez finalice la vigencia del contrato, según lo solicite el Responsable, y le corresponderá facilitar al Responsable toda la información que demuestre el cumplimiento de las instrucciones dadas por el

[95] Ibid. Art. 22. Núm. 2.
[96] Ibid. Art. 27.

Responsable y de las obligaciones estipuladas en el Contrato. Así mismo, el Encargado deberá contribuir con las auditorías o inspecciones y si se cree que se está infringiendo el Reglamento por la ejecución de alguna de las instrucciones recibidas, se debe informar al Responsable. El RGPD contempla que en caso de que se recurra a otro Encargado (subencargado), se deberá suscribir un contrato que contenga como mínimo, las mismas condiciones y obligaciones que suscribió con el Encargado con el Responsable.[97]

22. El Encargado deberá llevar un registro de todas las actividades llevadas a cabo para el tratamiento que contenga, por escrito y en formato electrónico[98]:

- Nombre y datos de contacto del Encargado o encargados, del Responsable, del representante del Responsable o el Encargado y del delegado de protección de datos.
- Categoría del tratamiento efectuado a los datos por cuenta del Responsable.
- Transferencia de los datos a terceros países, la identificación del país, y la documentación de las garantías que se implementarán.
- Descripción general de las medidas técnicas y organizativas de seguridad.

23. El Encargado debe garantizar que todas las personas que actúen bajos sus órdenes, sólo puedan tratar los datos a los que tendrán acceso, siguiendo las instrucciones dadas por el Responsable.[99]

24. El Encargado tiene la obligación de nombrar un delegado de protección de datos siempre que el tratamiento lo haga una autoridad u organismo público (a excepción del ejercicio de la función judicial), que una de las actividades principales del Encargado sea el tratamiento de datos que, de alguna u otra forma, podría requerir observación constante por parte de los interesados en

---

[97] Ibid. Art. 28.
[98] Ibid. Art. 30.
[99] Ibid. Art. 32. Núm. 4. RGPD, artículo 32, numeral 4.

masa, o ejecute el tratamiento de datos en masa de categorías especiales de datos o de infracciones penales. El Delegado deberá contar con conocimiento especializado en Derecho y con experiencia en protección de datos. Sus datos deben ser publicados y comunicados a la autoridad de control.[100] El delegado debe rendir cuentas al superior jerárquico de la compañía, y también está obligado a guardar estricta confidencialidad en el desempeño de sus funciones.[101]

Entre sus funciones están el colaborar y asesorar al Encargado y sus colaboradores, vigilar el cumplimiento del Reglamento y la ley vigente para el efecto, colaborar con la formación del personal con las auditorías, asesorar sobre la evaluación de impacto, cooperar con las autoridades y ser su contacto, entre otras.[102]

25. La certificación de la que se habló anteriormente, debe ser expedida por un órgano autorizado por los Estados miembros de la unión, el cual certificará con el *"Sello Europeo de Protección de Datos",* y tendrá una vigencia de tres años.[103]

26. A la luz de los requisitos que exige el Artículo 45 del Reglamento, la Comisión no ha considerado a Colombia de forma oficial, como un Estado que garantice un nivel de protección adecuado; sin embargo, es posible efectuar la transferencia de datos a Colombia, si el Encargado ofrece garantías adecuadas (las que se han mencionado a lo largo de este capítulo), y le permite a los interesados poder exigir sus derechos y adelantar acciones legales efectivas.[104] Si no se logra cumplir con lo anterior se podrá realizar la transferencia si los interesados tienen conocimiento de la misma y de los riesgos que se prevén, si por causa de un contrato a celebrarse o en ejecución entre los interesados y el

---

[100] Ibid. Art. 37. RGPD, artículo 37.
[101] Ibid. Art. 38. Núm. 3 y 5..
[102] Ibid. Art. 39.
[103] Ibid. Art. 42. Núm 5 y 7.
[104] Ibid. Art. 47..

Responsables es necesario realizarla, por razones de interés público, para formulación, ejercicio o defensa de reclamaciones, para proteger los intereses de los interesados en los casos en que estén incapacitados para dar su consentimientos, cuando se trate de información abierta al público cumpliendo las condiciones establecidas para su consulta, entre otros; y esto, sólo si el tratamiento no es repetitivo, que se trate de una cantidad limitada de interesados, que sus interés y derechos nunca sean inferiores al interés legítimo del Responsable, y de todas formar se ofrezcan garantías adecuadas.[105]

2.4.2. Sanciones estipuladas en el RGDP

1. Es facultativo de cada órgano de control de los estados Miembro, determinar las multas administrativas, y en qué medidas serán aplicadas, respondiendo siempre a principios de coherencia y a la tutela judicial efectiva.[106]

2. Se debe indemnizar a los interesados por todos los daños o perjuicios que se le puedan ocasionar, con fundamento a la violación de lo dispuesto en el Reglamento u otras normas sobre la materia. Cada Responsable o Encargado deberá responder por la totalidad de los daños, sin embargo, podrá dividirse la responsabilidad en atención a las actuaciones o participación de cada Parte.[107]

3. Cada Estado miembro establece las medidas para garantizar el cumplimiento del reglamento.[108]

4. Si un Encargado viola el Reglamento, al determinar medios y fines del tratamiento, se le considerará como Responsable del Tratamiento.[109]

---

[105] Ibid. Art. 49.
[106] Ibid. Pág. 28. Núm. 150..
[107] Ibid. Pág. 27. Núm. 146.
[108] Ibid. Art. 51.
[109] Ibid. Art. 28. Núm. 10..

5. Las autoridades de control podrán advertir al Encargado ante una presunta violación del reglamento, sancionarlo cuando se perciba la infracción, ordenar que atienda las solicitudes hechas por los interesados, ordenarle que sus operaciones se ajusten al Reglamento, que comunique al interesado las violaciones a la seguridad, limitar temporal o definitivamente el tratamiento, imponer multas administrativas, entre otros.[110]

6. Se deberá indemnizar a las personas por los daños y perjuicios sufridos con ocasión a la infracción del Reglamento. Aun así, el Encargado sólo será responsable de tales daños cuando haya incumplido alguna de las obligaciones del Reglamento dirigidas directamente a los Encargados o cuando haya violado las instrucciones legales del Responsable. Si el Encargado es declarado culpable y paga la indemnización debida, y si hay responsabilidad por parte del Responsable u otros Encargados, el Encargado que pagó la indemnización, podrá reclamar que cada uno pague lo proporcionado a su responsabilidad.[111]

7. Para la imposición y cálculo de multas, el ente de control tendrá en cuenta lo siguiente:[112]

- Naturaleza de la infracción y de la operación, gravedad, duración de la infracción, propósito de las operaciones de tratamiento, cantidad de interesados afectados y graduación de los daños ocasionados.
- Si hubo o no intención, y negligencia.
- Medidas para mitigar los daños.
- Grado de responsabilidad del Encargado.
- Infracciones que el Encargado haya cometido con antelación.
- Qué tanto cooperó con la autoridad de control para aliviar y mitigar los daños de la infracción.

---

[110] Ibid. Art. 58. Núm. 2. RGPD, artículo 58, numeral 2.
[111] Ibid. Art. 82.
[112] Ibid. Art. 83.

- Categoría de datos afectados.
- Si el Encargado notificó de la infracción a la autoridad, y de qué forma.
- Si cumplió con las medidas impuestas por la autoridad enunciadas en el numeral 5 anterior, si fueron ordenadas.
- Si se adhirió a algún código de conducta o está certificado por los organismos de certificación especificados en el artículo 43 del Reglamento.
- Algún otro factor atenuante o agravante, según el caso.

8. Si el Encargado actuó de forma negligente o intencional, el valor de la multa administrativa no será superior al valor más alto de la multa establecida para las infracciones más graves[113]. Hay multas hasta de 10.000.000 de Euros, o máximo el 2% del volumen del negocio total anual del ejercicio financiero del año inmediatamente anterior, para las causales establecidas en el numeral 4 del Artículo 83. Para los casos estipulados en el numeral 5 del Artículo 83, como los atinentes a los principios básicos del tratamiento, derechos de los interesados, transferencia de datos a un tercer país, incumplimiento de lo resuelto por una autoridad de control[114] y demás, las multas administrativas son hasta 20.000.000 de Euros, o máximo 4% del volumen del negocio total anual del ejercicio financiero del año inmediatamente anterior. En todos los casos se opta por una cuantía mayor. Cada Estado miembro podrá establecer de igual forma la cuantía de las multas administrativas, y las estipuladas en el Reglamento serán aplicables cuando un Estado miembro no lo haya establecido en su legislación propia.

2.5. NORMATIVIDAD APLICABLE A LA PROTECCIÓN DE DATOS PERSONALES EN ESTADOS UNIDOS

[113] Ibid. Art. 83. Núm 3.
[114] Ibid. Art. 83. Núm. 6.

En la legislación estadounidense, no es posible identificar una norma general sobre Protección de Datos, por lo tanto, se tiene establecido que cada estado federal tiene el deber de crear leyes para la protección de los consumidores y evitar prácticas fraudulentas en su contra, además de reforzar las regulaciones sobre privacidad y protección de los datos. Sin embargo, es posible observar una serie de normas de carácter federal, esto es, aplicable a todos los estados y de obligatorio cumplimiento, como es el caso del reglamento para la Protección de la Privacidad de los Conductores (DDPA, Act of 1994), el reglamento para la Protección de la Privacidad de los Niños en línea (COPPA), el relacionado con la Protección de la Privacidad de los Videos (VPPA), la Política de Comunicaciones por Cable (Cable Communications Policy Act 1984), la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, Acto 1996) que regula lo concerniente a la información médica individualmente identificable, su intercambio electrónico, las transacciones al respecto, entre otros asuntos, que, deben atender los distintos proveedores que presten servicio de atención médica y la cual resulta importante mencionar toda vez que debe ser tenida en cuenta por las compañías dedicadas a los servicios de Contact Center que pretenden prestar servicios orientados a la atención de cliente de entidades prestadoras de servicios de salud. Por otro lado, la Ley de Protección del Consumidor Telefónico (TCPA), regula la forma en la que se deben prestar los servicios de atención telefónica, como llamar en una franja horaria de 8 A.M. a 9 P.M., respetar la lista de *do-not-call,* además de que el agente que llame, se debe presentar, mencionar la compañía para la que trabaja y dar el número de teléfono de contacto, entre otros asuntos[115]. En Colombia, no hay una ley que regule en sí la forma en que se deben prestar los servicios de Contact Center, sin embargo, se han emitido regulaciones para controlar ciertos aspectos, por ejemplo, el artículo 7, literal h, de la Ley 1328 de 2009, menciona que las gestiones de cobro, deben hacerse en horarios adecuados, con el fin de evitar el hostigamiento, por otro lado, el proyecto de ley 519 de 2021, buscaba regular el horario de cobranza,

[115] RICHARDS, Francine. Regulations for Call Center Operations. Revista CHRON. https://smallbusiness.chron.com/regulations-call-center-operations-22076.html

para que se haga en días hábiles, de 8 A.M. a 6 P.M., sin embargo el proyecto se encuentra archivado.

Como se mencionó anteriormente, cada uno de los Estados en Estados Unidos, puede generar normas específicas en relación con la protección de datos y hasta el momento de la elaboración del presente trabajo, el de mayor importancia es el California Consumer Privacy Act (en adelante, CCPA), el cual está orientado en su mayor parte, a lo que tiene que ver con las obligaciones del Encargado del Tratamiento, y, sobre todo, al tratamiento de datos de quienes residan en California, y que deberá tenerse en cuenta en caso de que la Compañía preste servicios a este público.

2.5.1. Obligaciones sobre el tratamiento de datos desde el CCPA

1. El CCPA confiere al titular de los datos la facultad de controlar el uso de la información, pero algo que no se ha mencionado anteriormente, la facultad de controlar la venta de su información, lo cual se considera fundamental del derecho a la privacidad.[116]

2. El CCPA le reconoce a los titulares el derecho de conocer la información que de ellos se ha recolectado, saber si su información es vendida o divulgada y a quién, decidir sobre la venta o no de sus datos, acceder a su información personal, y que haya igualdad respecto de los servicios y de los precios, aun cuando haga ejercer sus derechos.[117]

3. El titular de los datos, o consumidor, podrá en todo momento solicitar su información personal sin costo, pero no podrá hacerlo más de dos veces en un período de 12 meses; y la empresa deberá facilitarlo en un formato que sea

---

[116] ESTADO DE CALIFORNIA. Califiornia Consumer Privacy Act (CCPA). Sec. 2, Lit. a. g
[117] Ibid. Sec. 2, Lit. i.

utilizable, en la medida de lo posible, para que el consumidor proporcione esa información a otra compañía.[118]

4. Una empresa no está en la obligación de conservar la información personal cuando se trate de una única transacción, de una sola vez, siempre que esa información no sea vendida o retenida por la empresa, o que sea identificable como información personal aunque no se haya mantenido para el efecto.[119]

5. Las empresas o proveedores, no estarán obligados a eliminar la información del consumidor, cuando este lo solicite, en los casos en que se requieran para completar una transacción o ejecución de un contrato; detectar incidentes de seguridad o enjuiciar a las personas responsables por fraude o actividades ilegales; identificar y reparar errores para garantizar funcionalidad; en ejercicio de la libertad de expresión; en cumplimiento de la Ley de Privacidad de Comunicaciones Electrónicas de California (*California Electronic Communications Privacy Act)*; investigaciones científicas, históricas o estadísticas públicas, y su eliminación podría poner en riesgo el fin de las mismas; para uso interno en atención a la relación con las empresas y los consumidores, o para uso de manera legítima compatible con el contexto en que la información fue proporcionada y para el cumplimiento de una obligación legal.[120]

6. El interesado podrá solicitar que se le informe, en caso de que su información haya sido vendida, las categorías de la información que vendieron de él, con propósito comercial o no, las categorías de aquellos a los que se les vendió la información. Un tercero no podrá vender información del interesado si fue vendida por una empresa, salvo que se le notifique al interesado y pueda ejercer su derecho de retracto[121], el CCPA lo menciona como "*right to opt out"* que

---

[118] Ibid. Sec. 1798.100, Lit. d.
[119] Ibid. Sec. 1798.100, Lit. e.
[120] Ibid. Sec. 1798.105, Lit. d.
[121] Ibid. Sec. 1798.115.

traducido al español, podría entenderse como el derecho de optar por no participar o, para efectos del presente documento, el derecho a decidir que su información no sea compartida con terceros[122], que puede ser ejercido no sólo ante los terceros que vendan su información, sino también ante las empresas.

Las empresas deben incluir en sus sitios Web un enlace claro, visible y de fácil acceso que diga “No vender mi información personal”, para que puedan ejercer su *“right to opt out”*.[123] Adicional a ello, deberá de respetar a los consumidores la decisión sobre su *“right to opt out”*, por lo menos durante 12 meses antes de volver a solicitar la autorización para vender su información.[124] El ejercicio de un consumidor del *“right to opt out”* debería implicar no solo la venta de su información, sino la transmisión de sus datos a cualquier título. Si bien esta es una obligación propia del Responsable o posible CLIENTE, en los casos en los que se encargue al PROVEEDOR el mantenimiento o desarrollo de páginas Web, el PROVEEDOR debe estar en la capacidad de implementar o crear este enlace, por lo que el conocimiento en la materia será de gran valor para el CLIENTE y sus consumidores.

7. Si bien el CCPA obliga a las empresas a informar al Consumidor que su información podría ser vendida[125], en resumidas cuentas, también le otorga la facultad a las empresas de vender la información que recolectan de una persona. Las empresas no podrán vender información de menores de 16 años, salvo consentimiento expreso de ellos (de los 13 a los 16 años), o de sus padres o tutores legales en caso de que sean menores a 13 años. Esta autorización se entenderá como *“right to opt in”,* que, traducido al español, podría entenderse como el derecho a participar o, para efectos del presente documento, el derecho

---

[122] Ibid. Sec. 1798.120, Lit. a.
[123] Ibid. Sec. 1798.135, Lit. a, Núm. 1.
[124] Ibid. Sec 1798.135, Lit. a, Núm. 5.
[125] Ibid. Sec. 1798.120, Lit. b.

decidir que su información sea compartida con terceros. Ignorar la edad de los consumidores, permitirá que se presuma que el consumidor ya la conocía.[126]

8. No se pueden ejercer medidas discriminatorias a los consumidores por haber ejercido sus derechos, y por tanto, las empresas no podrán, de forma deliberada, negar bienes o servicios, cobrar diferentes precios por bienes o servicios, imponer sanciones, proporcionar los bienes o servicios a un nivel o calidad diferentes.[127]

9. Respecto de la solicitud de información del titular, las empresas deben poner a disposición de este, por lo menos dos (2) medios para hacer la solicitud, bien sea teléfono, o correo electrónico, o los demás medios que la empresa considere pertinentes. Por otro lado, deberá responderse la solicitud dentro de los cuarenta y cinco (45) días siguientes a la fecha de recepción de la solicitud (no especifica si son días hábiles o calendario, pero se recomienda tomarlos como calendario), los cuales podrán prorrogarse por cuarenta y cinco (45) días más, siempre que se le avise al titular de la extensión del plazo. La información que se entregue del titular, deberá contener toda la información recopilada de él durante los doce (12) meses anteriores a la fecha de solicitud, por el medio elegido por el titular para recibir la información.[128]

10. Las políticas de protección de la privacidad de los consumidores, se deben actualizar por lo menos una vez cada año, en ellas se deben enumerar los derechos del consumidor, los medios para que él pueda presentar solicitudes, hacer una lista de las categorías de datos que recopilan de él.[129] En sus sitios Web, deben facilitar un enlace que permita a los consumidores consultar sus

---

[126] Ibid. Sec, 1798.120, Lit. d.
[127] Ibid. Sec. 1798.125, Lit. a.
[128] Ibid. Sec. 1798.130. Núm. 2.
[129] Ibid. Sec. 1798.130. Núm. 5.

políticas de privacidad y se debe hacer mención de los derechos de privacidad de los consumidores de California.[130]

11. El CCPA, incluye, dentro de lo que se entiende como *información personal*, aquella que se refiere a la actividad en internet, como historial de navegación o búsqueda, su interacción en un sitio web, aplicación o con un anuncio en internet[131], también comprende los datos de geolocalización[132].

2.5.2. Sanciones estipuladas en el CCPA

1. El CCPA instruye al consumidor, para que, antes de interponer una acción penal, notifique al Encargado o Responsable del tratamiento, para que, dentro de los treinta (30) días siguientes a la fecha de notificación, se pronuncie frente a los hechos que representan la violación de las disposiciones sobre la privacidad de los datos, con el fin de que el Encargado o Responsable encuentre una posible solución, de ser así, y de poderse subsanar, el consumidor se debe abstener de presentar una acción en contra de la Compañía en cuestión.[133]

2. En las sanciones civiles que se contemplan por la violación de la norma, se evaluarán en atención al caso en específico, y atendiendo a situaciones como la naturaleza de la infracción, la gravedad, la cantidad de infracciones y su persistencia en el tiempo, la intencionalidad, y el patrimonio de la compañía que comete la infracción[134], dichas sanciones podrían ser que se condene a una Compañía a resarcir daños que puedan ir de los $100 a los $750 dólares estadounidenses, la declaración de medidas cautelares, o la imposición de cualquier otra reparación que el tribunal declare.[135]

---

[130] Ibid. Sec. 1798.135, Núm. 2.
[131] Ibid. Sec. 1798.140, Lit. o, Núm. 1, sub literal F.
[132] Ibid. Sec. 1798.140, Lit. o, Núm. 1, sub literal G.
[133] Ibid. Sec. 1798.150. Lit. b. Núm. 1.
[134] Ibid. Sec. 1798.150. Lit. a, Núm 2.
[135] Ibid. Sec. 1798.150. Lit. a, Núm 1.

3. Además de las sanciones que, por disposición de la ley, se pueden imponer, también se podrán imponer sanciones que podrán ser hasta por siete mil quinientos dólares estadounidenses (USD $7.500), por cada infracción.[136]

2.6. RESPONSABILIDAD DE EMPRESAS DE CONTACT CENTER COMO PROVEEDORES DEL SERVICIO

En un comienzo, los servicios que prestaban los Call Center, eran estrictamente de llamadas, cuyos inicios datan en la década de los 60, actualmente, los Centros de Contacto han apuntado por ofrecer un servicio integral, que pueda acercar a los usuarios y empresas de una forma más sencilla y cómoda, y esto, claro está, ha sido impulsado por el desarrollo tecnológico, que vertiginosamente ha incrementado, modificando las formas en las que se hacen negocios, compras y demás. Teniendo esto en cuenta, podemos ver que ahora los centros de contacto se encuentran en la capacidad de administrar las redes sociales de sus clientes, y, por tanto, recibir y hacer interacciones por medio de ellas; por otro lado, están en capacidad de recibir solicitudes por medio de un chat en la página web de sus clientes, y así efectuar la solicitud de un servicio, cancelar un servicio o simplemente recibir información. Todas estas actividades conllevan en sí diversos riesgos, como el ciber ataque, el posible fraude que pueda cometer un colaborador, una falla en la tecnología que se use, daños en las redes de internet, fallas en las plataformas, como WhatsApp (cuyo correcto funcionamiento es atribuible a Facebook – ahora Meta –, y no al prestador de servicios de Contact Center), entre otros, riesgos que pueden ser previsibles y otros que no, unos requerirán de la diligencia del proveedor para prevenirlos y otros, simplemente, se escapan del control humano, y la ocurrencia de esos hechos, ocasionaría que sobre la cabeza del proveedor recaiga el deber de responder por los perjuicios

[136] Ibid. Sec. 1798.155. Lit. b.

que puedan ocasionar, y es por esta razón que se deben establecer cláusulas claras para evitar pleitos costosos y desgastantes.

El artículo 2341 del Código Civil colombiano, establece que todo el que haya cometido un daño debe indemnizar al afectado, además de las sanciones que la ley le imponga, en ese mismo sentido, el artículo 2356 del mismo código estipula que todos los daños causados por malicia o con negligencia deben ser reparados, por otra parte, el artículo 167 del Código General del Proceso, estipula, que "*Incumbe a las partes probar el supuesto de hecho de las normas que consagran el efecto jurídico que ellas persiguen*", sin embargo, el juez estará en la capacidad de trasladar la carga de la prueba si considera que la otra parte podría aportar las pruebas con mayor facilidad; considerando esto, es necesario que toda cláusula que esté orientada a la responsabilidad o resarcimiento de daños, se limite a que toda responsabilidad atribuible al proveedor sea debidamente probada, que el proveedor pueda contar con la oportunidad de conocer el hecho por el cual le podría multar o cobrar alguna indemnización, y que además, pueda controvertir los hechos que en su contra se alegan, todo esto en la etapa contractual, y que, en caso de no llegar a un acuerdo, sea un juez de la República quien se encargue de decidir al respecto, aunque para clientes internacionales, esto último podría variar.

Uno de los mecanismos que contractualmente suele usarse para asegurar la indemnización de perjuicios es la constitución de pólizas de seguro que respalden el cumplimiento de la prestación del servicio, y de otros riesgos inherentes a él, aunque para efectos del presente trabajo no se ahonda en los contratos de seguros, sólo se menciona como una alternativa conveniente a añadir al momento de la suscripción de contratos.

Según el RGPD, podrá probarse que el Encargado no violó lo establecido en las normas respecto del tratamiento y así evitar la responsabilidad y el deber de

indemnizar al interesado.[137] El Encargado será exento de responsabilidad si logra demostrar que no es responsable de los hechos que ocasionaron el daño.[138] En estos supuestos, se puede concluir que la carga de la prueba recae exclusivamente en el Encargado, es decir en el PROVEEDOR, es por ello, que el RGPD exige que todas las medidas tendientes a dar cumplimiento a lo reglamentado, sean debidamente documentadas y puedan ser demostradas. Asimismo, el RGPD, contempla que no se aplicaría tal reglamento en los escenarios de seguridad nacional, política exterior y seguridad común de la Unión Europea[139], adicionalmente, no se deberá aplicar el Reglamento, cuando se trate de información anónima, siempre y cuando, esa información no pueda atribuirse a una persona física directa o indirectamente[140].

Finalmente, cómo se mencionó anteriormente, en el CCPA, el Encargado tendrá la posibilidad de evitar una acción en su contra, si, dentro de los treinta (30) días siguientes a la notificación del titular afectado, se revisan las situaciones que dieron lugar al incumplimiento y se subsanan, evitando un daño, eso, si el daño aún no se ha ocasionado; lo que resultaría también recomendable establecer como procedimiento previo a la imposición de multas, que el PROVEEDOR, ante la notificación de una posible afectación o riesgo a la privacidad de los datos de un titular, pueda ejecutar todas las acciones tendientes a evitar el daño, por lo que la multa sólo se haría efectiva en el caso en que el daño se haya materializado, además de que, se haya comprobado que fue ocasionado por las acciones u omisiones del Proveedor.

2.7. FORMATO DE CUMPLIMIENTO

[137] Op. Cit. RGPD, Pág. 27, Núm. 146.
[138] Ibid. Art. 82, Núm. 3.
[139] Ibid. Pág. 3, Núm. 16.
[140] Ibid. Pág. 5. Núm. 26.

Con el fin de aportar una guía práctica para el cumplimiento de los diferentes reglamentos y recomendaciones recogidas a lo largo del presente trabajo, se anexa una plantilla que contiene los ítems principales que se deberían tener en cuenta para la implementación de las normas en materia de protección de datos dentro de las organizaciones especializadas para la prestación de servicios de Contact Center y BPO.

Tabla 5. Formato de Cumplimiento.

ORIGEN	NORMA	REQUISITO	RESPONSABLE	PORCENTAJE DE CUMPLIMIENTO	OBSERVACIONES
Colombia	Ley 1266 de 2008, artículo 7, numerales 1, 7, 8. Ley 1581, artículo 17, literal a.	La Compañía proporciona al titular los canales necesarios para la presentación de sus peticiones, quejas o solicitudes.			
Colombia	Ley 1266 de 2008, artículo 7, numeral 4. Ley 1581 de 2012, artículo 17, literal k, artículo 18, literal f. Decreto 1377 de 2013, artículo 13.	La Compañía tiene políticas y procedimientos establecidos para dar trámite a las peticiones, quejas o solicitudes presentadas por los titulares, bajo los parámetros establecidos por ley.			
Colombia	Decreto 1377 de 2013, artículos 14 y 15.	La Política de Privacidad de los Datos es dada a conocer al titular.			
Colombia	Ley 1266 de 2008, artículo 7, numeral 3. Ley 1581 de 2012, artículo 17, literal d, artículo 18, literal b.	La información de los titulares es resguardada con la seguridad necesaria para proteger su confidencialidad.			
Colombia	Ley 1266 de 2008, artículo 7, numeral 6.	La Compañía cuenta con la infraestructura física y tecnológica adecuada para garantizar que el almacenamiento de la información sea seguro.			
Colombia	Ley 1266 de 2008, artículo 7, numeral 5. Ley 1581 de 2012, artículos 10 y 17, literal b.	La Compañía tiene un procedimiento establecido para obtener la autorización de los titulares para el tratamiento de su información y conserva la prueba necesaria para soportar dicha autorización, salvo los casos exceptuados por ley.			
Colombia	Ley 1581 de 2008, artículo 18, literal d.	La Compañía efectúa o escala la actualización de los datos del titular dentro de los 5 días hábiles establecidos en la ley, una vez hecha la solicitud.			
Colombia	Ley 1266 de 2008, artículo 8, numeral 6. Circular Única de la Superintendencia de Industria y Comercio, Título V, numeral 1.2.	La Compañía solicita a sus clientes la certificación en la que den cuenta de la autorización para el tratamiento de la información proporcionada a la Compañía para la ejecución del objeto del Contrato.			
Colombia	Ley 1266 de 2008, artículo 11.	La Compañía tiene un área destinada exclusivamente para la recepción de peticiones y reclamos sobre los datos personales.			
Colombia	Ley 1266 de 2008, artículo 16, numeral 2. Ley 1581 de 2012, artículo 15.	La Compañía escala las peticiones, quejas y reclamos, dentro de los dos (2) días hábiles siguientes a los días de recepción, para que el Cliente atienda la reclamación dentro de los términos de ley.			
Colombia	Decreto 1377 de 2013, artículo 4.	Al momento de recolección de la información, sólo se recolectan los datos necesarios para la finalidad que se pretende conseguir.			
España	RGPD, numeral 80.				
Colombia	Decreto 1377 de 2013, artículo 5.	La autorización para el tratamiento se obtiene al momento de la recolección.			
		Se informa al titular de forma oportuna en caso de que las finalidades para la que son recolectos los datos sufran un cambio, o que cambie la identificación del Responsable.			
Colombia	Decreto 1377 de 2013, artículo 7.	La Compañía garantiza la consulta de la autorización otorgada por el Titular.			
		La autorización otorgada por el Titular se obtiene por medios válidos, de forma inequívoca y entendible.			

Colombia	Decreto 1377 de 2013, artículo 11.	La Compañía tiene documentado todos los procesos implementados para el tratamiento.			
Colombia	Decreto 90 de 2018, artículo 1.	La Compañía está inscrita en el Registro Nacional de Bases de Datos. (Aplicable para entidades con activos totales superiores a los 100.000 UVT).			
Colombia	Decreto 1074 de 2015, Art. 2.2.2.25.2.8.	La Compañía garantiza el borrado seguro de los datos que deben ser suprimidos o eliminados.			
Unión Europea	RGPD, numeral 15.	La Compañía garantiza que la tecnología o técnicas automatizadas usadas para el tratamiento de los datos es monitorizada y actualizada por medio de personal calificado.			
Unión Europea	RGPD, numeral 56.	La Compañía garantiza la pseudonimización de los datos.			
Unión Europea	RGPD, numeral 43.	El titular tiene la capacidad de otorgar su autorización a cada finalidad de manera separada.			
Unión Europea	RGPD, numeral 75.	La Compañía cuenta con una matriz de riesgos donde se identifican los posibles riesgos que puedan ocurrir, su probabilidad y gravedad.			
Unión Europea	RGPD, numeral 90.	La Compañía establece medidas encaminadas a mitigar los riesgos y garantizar la protección de la información.			
Unión Europea	RGPD, artículo 35, numeral 7.	La Compañía realiza la respectiva evaluación de impacto a los datos personales a los que dará tratamiento.			
Unión Europea	RGPD, numeral 98.	La Compañía cuenta con un Código de Conducta para dar cumplimiento al RGPD.			
Unión Europea	RGPD, artículo 1, numeral 2, y artículo 30.	La Compañía aporta las evidencias suficientes para demostrar el cumplimiento de las obligaciones contenidas en el RGPD.			
Unión Europea	RGPD, atículo 7, numeral 3.	El titular tiene la posibilidad de retirar su autorizacíon con la misma facilidad con que puede otorgarla.			
Colombia	Ley 1266 de 2008, artículo 16, numeral 1. Ley 1581 de 2012, artículo 14.	La Compañía cumple con los términos establecidos para la atención de solicitudes.			
Unión Europea	RGPD, artículo 12, numeral 4.				
Estado de California (EEUU)	CCPA, Sección 1798.130., numeral 2.				
Estado de California (EEUU)	CCPA, Sección 1798.130., numeral 5.	La Compañía actualiza sus políticas por lo menos una vez al año.			
Estado de California (EEUU)	CCPA, Sección 1798.135, Literal a, Numeral 1.	La Compañía en su página web, tiene publicado el enlace, de manera visible, para que el titular de la información ejerza el *right to opt out*.			
Estado de California (EEUU)	CCPA, Sección 1798.130. Numeral 2.	La Compañía pone a disposición de los titulares, dos medios o más, para la presentación de solicitudes, quejas o reclamos.			

3. TERCERA PARTE

3.1. CONCLUSIONES

La recopilación normativa de los diferentes órdenes jurídicos abordados, permite dilucidar una mayor o menor rigurosidad de tales órdenes ante la protección de datos personales, y, a pesar de que un ordenamiento jurídico sea muy diferente del otro, resultará satisfactorio el poder tomar elementos tanto de la reglamentación europea como de la reglamentación estadounidense y poder complementarlo con la forma en la que actualmente, se deben tratar los datos, se prestan los servicios y se suscriben contratos. Es imperante recordar que cada organización tiene el deber mantener actualizados en los avances y cambios normativos en la materia, pero este trabajo monográfico está orientado a informar a las compañías de prestación de servicios de Contact Center sobre la normatividad actual en materia de protección de datos, y brindarle un lineamiento para llevar a cabo su cumplimiento a la hora de prestar sus servicios a sus clientes, y los usuarios de sus clientes, puesto que hasta el momento no se cuenta con una ley específica en Colombia que defina como tal la forma en la que se deben prestar los servicios en los centros de contacto, y teniendo en cuenta que además, la tecnología seguirá desarrollándose de forma vertiginosa, y con ello, las capacidades y formas de conectar con las personas y las empresas.

La legislación extranjera, como es de esperarse y sucede también con la colombiana, no contempla condiciones o requerimientos específicos para el tratamiento de los datos por fuera del ámbito territorial de la ley, lo cual pone un poco en aprietos y dificulta la aplicación de las normas para quien desde afuera pretende tratar lo datos personales desde un país externo al país de la norma.

3.2. BIBLIOGRAFÍA

CONGRESO DE LA REPÚBLICA. Ley 454 de 1998. Diario oficial No. 43.357.

CONGRESO DE LA REPÚBLICA. Ley 1266 de 2008. Diario Oficial No. 47.219.

CONGRESO DE LA REPÚBLICA. Ley 1581 de 2012, Diario Oficial No. 48.587

CORTE CONSTITUCIONAL. Sentencia C-651 del 3 de diciembre de 1997. Magistrado Ponente Carlos Gaviria Díaz

CORTE CONSTITUCIONAL. Sentencia C-263/2011, 6 de abril de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

CORTE CONSTITUCIONAL. Sentencia T-176A/2014, 25 de marzo de 2014. M.P. Jorge Ignacio Pretelt Chaljub.

COUNCIL OF EUROPE. Colombia: Un primer paso hacia el Convenio. 30 de Agosto de 2019. [Online] https://www.coe.int/es/web/data-protection/-/colombia-a-first-step-towards-convention-108-

ESTADO DE CALIFORNIA. Califiornia Consumer Privacy Act (CCPA).

PORTAFOLIO. La profesionalización de los Contact Center. 20 de junio de 2016. En: Revista Portafolio [Online] https://www.portafolio.co/evolucion-contact-centers-colombia-revista-portafolio-497791

PRESIDENCIA DE LA REPÚBLICA. Decreto 1727 de 15 de mayo de 2009. Diario Oficial No. 47350.

PRESIDENCIA DE LA REPÚBLICA. Decreto 1377 de 27 de junio de 2013. Diario Oficial No. 48834.

PRESIDENCIA DE LA REPÚBLICA. Decreto 886 de 13 de mayo de 2014. Diario Oficial No. 49150

PRESIDENCIA DE LA REPÚBLICA. Decreto 1074 de 26 de mayo de 2015. Diario Oficial No. 49523.

RICHARDS, Francine. Regulations for Call Center Operations. Revista CHRON. https://smallbusiness.chron.com/regulations-call-center-operations-22076.html

SECRETARÍA GENERAL DEL SENADO. Constitución Política de Colombia (Gaceta Constitucional No. 116 de 20 de julio de 1991).

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Circular única. Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/Titulo%20V%20Proteccion_Datos_Personales.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 71307 de 28 de noviembre de 2014.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 8483 de 27 de febrero de 2014.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 58969 de 29 de septiembre de 2014.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 6074 de 18 de marzo de 2019

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 17629 de 29 de mayo de 2019.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 17629 de 29 de mayo de 2019.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 64328 de 19 de noviembre de 2019.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 38281 de 14 de julio de 2020.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 77049 de 30 de noviembre de 2020.

UNIÓN EUROPEA. Reglamento General de Protección de Datos. 24 de mayo de 2018. Referencia DOUE: L 119, 4.5.2016,.