GUÍA SOBRE EL TRATAMIENTO DE DATOS PERSONALES PARA FINES DE COMERCIO ELECTRÓNICO

DELEGATURA PARA LA PROTECCIÓN DE DATOS PERSONALES

2019

El futuro es de todos

Gobierno de Colombia

Industria y Comercio

SUPERINTENDENCIA

Industria y Comercio
SUPERINTENDENCIA

GUÍA SOBRE EL TRATAMIENTO DE DATOS PERSONALES

PARA FINES DE COMERCIO ELECTRÓNICO

DELEGATURA PARA LA PROTECCIÓN DE DATOS PERSONALES

El futuro es de todos
Gobierno de Colombia

TABLA DE CONTENIDO

TABLA DE CONTENIDO

INTRODUCCIÓN

El comercio electrónico es el motor de la economía del siglo XXI y los datos personales son la moneda de la economía digital. El primero hace referencia a "la realización de actos, negocios u operaciones mercantiles concertados a través del intercambio de mensajes de datos telemáticamente cursados entre proveedores y los consumidores para la comercialización de productos y servicios"[1] o a las "cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar"[2] . El desarrollo de las actividades que abarca el comercio electrónico implica la recolección, uso o circulación de sus datos personales.

Respecto de la protección del consumidor en el comercio electrónico, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha recomendado lo siguiente sobre privacidad y seguridad:

> ***"48. Las empresas deberían proteger los datos personales del consumidor, asegurándose de que sus prácticas relacionadas con la recopilación y el uso de datos del consumidor sean legales, transparentes y justas, y que permitan la participación y elección del consumidor y tomen precauciones de seguridad razonables.***
> ***49. Las empresas deberían gestionar el riesgo relacionado con la seguridad digital e implementar medidas de seguridad para reducir o mitigar los efectos adversos relacionados con la participación del consumidor en el comercio electrónico."[3]***

Según nuestra Constitución Política, *"el ejercicio de los derechos y libertades (...) implica responsabilidades"*[4] . Adicionalmente, *"la actividad económica y la iniciativa privada son libres, dentro de los límites del bien común"*[5] y, *"la empresa, como base del desarrollo, tiene una función social que implica obligaciones"*. Algunas de esas obligaciones son cumplir la Constitución Política y las leyes[6], así como "respetar los derechos ajenos y no abusar de los propios".

1. Cfr. Artículo 49 de la Ley 1480 de 2011
2. Cfr. Literal b) del artículo 2 de la Ley 527 de 1999
3. OECD (2016), OECD Recommendation of the Council on Consumer Protection in E-Commerce, OECD Publishing, Paris, https://doi.org/10.1787/9789264255258-en.

En esa medida, cualquier actividad de comercio electrónico debe ser respetuosa de, entre otros, lo que ordena el artículo 15 de la Carta Política, según el cual "en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución". La Ley Estatutaria 1581 de 2012 desarrolló este mandato constitucional y fue redactada de manera neutral tecnológica y temáticamente, razón por la cual aplica a cualquier tratamiento de datos independientemente de su finalidad. Asimismo, está al margen de las herramientas técnicas y/o científicas que se utilicen para dicho efecto.

Es importante tener presente que ni la Constitución ni la ley se oponen al tratamiento de datos para fines de comercio electrónico. Las dos solo exigen el cumplimiento de unas garantías mínimas adecuadas, a fin de no desatender, desconocer o vulnerar los derechos de las personas cuando, para realizar dichas actividades, se usan los datos de las personas.

4. Cfr. Artículo 95 de la Constitución Política de la República de Colombia.
5. Cfr. Artículo 333 de la Constitución Política de la República de Colombia.
6. Cfr. Artículos 6 y 95 de la Constitución Política de la República de Colombia.

OBJETIVOS Y PRECISIONES

Esta guía[7] tiene como propósito presentar algunas sugerencias a quienes utilizan datos personales para realizar actividades de comercio electrónico, con el fin de orientarlos para que desde el diseño de cualquier actividad o gestión se tengan en cuenta las exigencias de las regulaciones sobre Tratamiento de Datos Personales.

Son muchos los aspectos que involucra el comercio electrónico por lo que este texto solo hará referencia a uno de ellos. Es decir, al Tratamiento de Datos Personales en el contexto de esas actividades, el cual comprende cualquier gestión que se realice con dicha información, como la recolección, el almacenamiento, el uso, la circulación, el análisis, la indexación, etc.

Estas recomendaciones tienen un enfoque preventivo con miras a que una empresa directamente *(Responsable del Tratamiento)* o, a través de terceros *(Encargado del Tratamiento),* evite vulnerar los derechos de cualquier persona o cliente *(Titular del dato)* en el escenario del comercio electrónico.

Este documento no es un concepto legal, ni constituye asesoría jurídica. Tampoco pretende ser un listado exhaustivo de recomendaciones específicas sobre todos los temas que involucra el comercio electrónico, pues ello es un asunto interno de cada organización, conforme con los objetivos empresariales y en atención a la magnitud de cada uno de sus proyectos.

Las orientaciones contenidas en este texto solo comprenden algunos de los temas más relevantes sobre Tratamiento de datos en el comercio electrónico. Por consiguiente, el lector debe tener claro que este documento no incluye todos los deberes legales sobre la materia y que la omisión de algunos de ellos en esta guía no lo exime de cumplir todos los requerimientos jurídicos.

7. Para la elaboración de esta guía se siguió el formato y se usaron contenidos de: Red Iberoamericana de Protección de Datos (2019) - Recomendaciones generales para el Tratamiento de Datos Personales en la Inteligencia Artificial.

RECOMENDACIONES

I *Cumplir las normas locales sobre Tratamiento de Datos Personales (TDP) cuando su proyecto de comercio electrónico tiene efectos en varios países o utiliza datos de personas ubicadas en diferentes partes del mundo*

Aunque cada día el mundo es más transfronterizo, global e hiperconectado, ello no significa que las normas nacionales sobre Tratamiento de Datos Personales hayan desaparecido o que no sean de obligatorio cumplimiento. Por eso, para que su proyecto de comercio electrónico no sea objetado o cuestionado jurídicamente es muy relevante que desde el inicio realice un estudio de riesgos legales de las regulaciones nacionales.

Lo anterior, le permitirá definir una estrategia inteligente para, entre otras cosas; (i) mitigar dichos riesgos, (ii) ganar y mantener la confianza de los consumidores, (iii) no afectar la buena reputación de su organización, y (iv) evitar eventuales investigaciones de las autoridades de protección de datos o de otras entidades.

II *Implementar estrategias de Responsabilidad Demostrada (accountability) frente al Tratamiento de Datos Personales (TDP) para fines de comercio electrónico*

Desde el inicio, su organización debe establecer la manera como probará que ha adoptado medidas útiles para cumplir las reglas sobre el Tratamiento de datos. Es necesario tener presente que *"los responsables del Tratamiento de Datos Personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012"*[8] y en el Decreto 1377 de 2013. (Incorporado en el Decreto 1074 de 2015)

Medidas "apropiadas" son aquellas ajustadas a las necesidades del Tratamiento de datos Y "efectivas" son las que permiten lograr el resultado o efecto que se desea o espera. En otras palabras, no se deben adoptar medidas inoperantes, inservibles, inanes o infructuosas. Solo se deben instaurar aquellas adecuadas, correctas, útiles, oportunas y eficientes con el propósito de cumplir los requerimientos legales para realizar Tratamiento de Datos Personales.

8. Cfr. Artículo 26 del Decreto 1377 de 2013. (Incorporado en el Decreto 1074 de 2015)

Es preciso resaltar que la regulación sobre datos personales impone cargas probatorias en cabeza de los Responsables del Tratamiento como las siguientes:

a) Conservar prueba de haber informado al titular, al momento de solicitarle la autorización, de manera clara y expresa lo que ordena el artículo 12 de la Ley 1581 de 2012 y, cuando el Titular lo solicite, entregarle copia de ello[9]

b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular[10].

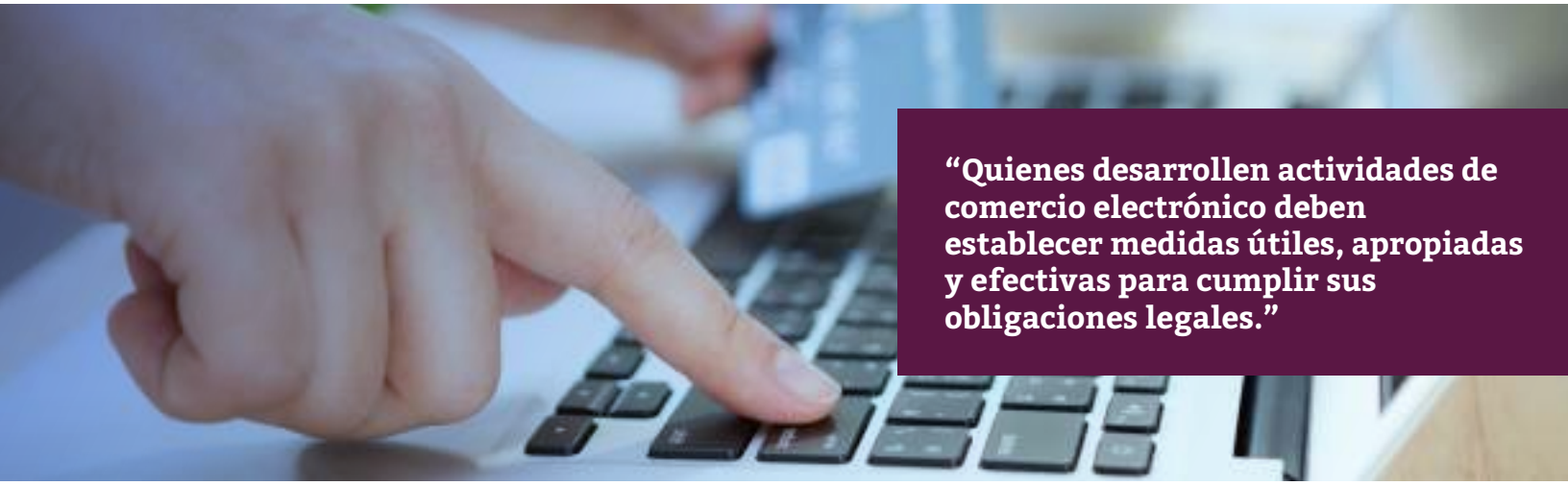
c) Proveer una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de información, como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso[11].

d) Documentar los procedimientos para el Tratamiento, conservación y supresión de los datos personales de conformidad con las disposiciones aplicables a la materia de que se trate[12].

e) Desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas[13].

f) Conservar el modelo del Aviso de Privacidad que utilicen para cumplir con el deber que tienen de dar a conocer a los Titulares la existencia de políticas del tratamiento de la información y la forma de acceder a las mismas, mientras se traten datos personales conforme al mismo y perduren las obligaciones que de este se deriven[14].

g) Adoptar las medidas razonables para asegurar que los datos personales que reposan enlasbases de datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando el Responsable haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento[15].



"Quienes desarrollen actividades de comercio electrónico deben establecer medidas útiles, apropiadas y efectivas para cumplir sus obligaciones legales."

9. Cfr. Parágrafo del artículo 12 de la Ley 1581 de 2012.
10. Cfr. Literal (b) del artículo 17 de la Ley 1581 de 2012 y artículo 8 del Decreto 1377 de 2013 "Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos".11. Cfr. Artículo 4 del Decreto 1377 de 2013.
12. Cfr. Artículo 11 del Decreto 1377 de 2013.
13. Cfr. Artículo 13 del Decreto 1377 de 2013.
14. Cfr. Artículo 16 del Decreto 1377 de 2013.
15. Cfr. Artículo 22 del Decreto 1377 de 2013.

En suma, quienes desarrollen actividades de comercio electrónico deben establecer medidas útiles, apropiadas y efectivas para cumplir sus obligaciones legales. Adicionalmente, tendrán que evidenciar y demostrar el correcto cumplimiento de sus deberes. Dichas herramientas, deben ser objeto de revisión y evaluación permanente, a fin de determinar su nivel de eficacia en cuanto al cumplimiento y grado de protección de los datos personales.

El reto de las organizaciones frente al Principio de Responsabilidad Demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas. Se trata de una actividad constante que exige demostrar un cumplimiento real y efectivo en la práctica de sus labores. No basta hacer declaraciones simbólicas de buenas intenciones, sino que es obligatorio evidenciar resultados concretos respecto del debido Tratamiento de los datos personales en los proyectos de comercio electrónico.

Es esencial realizar entrenamientos periódicos y especializados al equipo humano de la organización para proveerle la experticia, guía y herramientas que requiere para el correcto desarrollo de las tareas que involucren cualquier Tratamiento de Datos Personales.

III *Exigir el respeto de la Política de Tratamiento de Datos Personales a los terceros que contrata para realizar actividades de comercio electrónico*

Si su empresa *(Responsable del Tratamiento)* contrata a otra empresa o a un tercero *(Encargado del Tratamiento)* para realizar actividades de comercio electrónico, exíjale el cumplimiento de su Política de Tratamiento de Datos Personales y los deberes legales que esto conlleva. Con todo, no solo es obligatorio el desarrollo de sus políticas para el Tratamiento de los datos personales, también debe velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas[16].

Recuerde que esos terceros obran en nombre suyo y que usted responde frente a los Titulares de los datos y las autoridades por los errores o negligencia de ellos. Además, la ley les impone a estos la obligación de cumplir una serie de deberes[17].

No pierda de vista que esos terceros actúan en su nombre frente a sus clientes y que, según se haya acordado, ellos tienen acceso a una parte o a la totalidad de sus bases de datos.

IV *Efectuar estudios de impacto de privacidad*

16. *Cfr. Artículo 13 del Decreto 1377 de 2013.*
17. *Los deberes de los Encargados están previstos en el artículo 18 de la Ley 1581 de 2012.*

Previo al diseño y desarrollo del proyecto de comercio electrónico y en la medida en que sea probable que el mismo entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los Titulares, se sugiere efectuar una evaluación de impacto en la privacidad *(Privacy Impact Assessment - PIA por sus siglas en inglés),* con el fin de poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos para garantizar que los datos se tratarán debidamente y conforme con la regulación existente. Dicha evaluación debería incluir, como mínimo, lo siguiente:

- Una descripción detallada de las operaciones de Tratamiento de Datos Personales que involucra el proyecto de comercio electrónico.

- Una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los datos personales. La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos, son elementos cardinales del Principio de Responsabilidad Demostrada.

  Es fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un *"sistema de administración de riesgos asociados al Tratamiento de Datos Personales"* [18] que les permita *"identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales"*[19].

- Las medidas previstas para afrontar los riesgos, incluidas garantías, controles de seguridad, diseño de software, tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los Titulares de los datos y de otras personas eventualmente afectadas.

Los resultados de este estudio, junto con las estrategias para mitigar los riesgos, hacen parte de la aplicación del principio de privacidad desde el diseño y por defecto.

V *Incorporar la privacidad y la ética desde el diseño y por defecto*

La privacidad desde el diseño y por defecto *(Privacy by Design and by Default)* es considerada una medida proactiva para cumplir con el Principio de Responsabilidad Demostrada. Al introducir la privacidad desde el diseño se está buscando garantizar el correcto Tratamiento de los datos utilizados en los proyectos de comercio electrónico. La mejor manera de garantizar el debido Tratamiento de datos es tomando la privacidad como un componente esencial del diseño y puesta en marcha del proyecto de comercio electrónico.

18. Superintendencia de Industria y Comercio (2015) "Guía para implementación del principio de responsabilidad demostrada (accountability)". Págs 16-18.
19. Ibid. Pág. 16

La Privacidad por Diseño *"promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo [sic] por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización"*[20]. Por eso, desde antes que se recolecte información y durante todo el ciclo de vida de la misma, se deberían adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana y procedimental, entre otras) con el objeto de evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información, así como fallas de seguridad o indebidos Tratamientos de datos personales.

La ética desde el diseño y por defecto debe irradiar el esquema, desarrollo y uso de los datos en proyectos de comercio electrónico, teniendo que ser parte del ADN de cualquier aspecto relacionado con esa actividad.

20. Cfr. Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales. Disponible en: http://-mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf http://mediasco-pe.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf

VI *Evitar la suplantación de identidad de los consumidores*

El artículo 50 de la ley 1480 de 2011 **(Estatuto del Consumidor)** señala lo siguiente:

"Sin perjuicio de las demás obligaciones establecidas en la presente ley, los proveedores y expendedores ubicados en el territorio nacional que ofrezcan productos utilizando medios electrónicos, deberán:(...) "

e) "Mantener en mecanismos de soporte duradero la prueba de la relación comercial, en especial de la ***identidad plena del consumidor,*** *(...) de tal forma que garantice la integridad y autenticidad de la información y que sea verificable por la autoridad competente, por el mismo tiempo que se deben guardar los documentos de comercio". (Destacamos)"*

Suplantar significa, entre otras, ***"sustituir ilegalmente a una persona u ocupar su lugar para obtener algún beneficio"***[21]. La suplantación de identidad consiste en hacerse pasar por otra persona para diversos propósitos: engañar a terceros, obtener bienes y servicios con cargo a la persona suplantada, incurrir en fraudes y otros tipos de conductas ilícitas.

Mediante la suplantación de identidad los impostores obtienen créditos, adquieren productos o servicios en nombre de la persona suplantada y ésta última es la afectada porque, en muchos casos, le toca asumir el pago de dichas obligaciones. Con esto, desde la perspectiva del Tratamiento de Datos Personales, se observa que se vulneran, por lo menos y según el caso, los principios de veracidad y seguridad.

Se infringe el principio de veracidad porque la información tratada, difundida o reportada sobre una deuda adquirida por un suplantador no es veraz respecto de la persona suplantada ya que ella no fue quien adquirió dicha obligación. Esos datos inducen a error porque faltan a la realidad y presentan como obligada o morosa a una persona respecto de una deuda que no adquirió. Recuérdese que el tratamiento de este tipo de datos está proscrito por nuestra regulación. Nótese que tanto la Ley 1266 de 2008 como la Ley 1581 de 2012 expresamente prohíben *"el registro y divulgación de datos (...) que induzcan a error"*[22] o el *"tratamiento de datos (...) que induzcan a error"*[23] y que el principio de veracidad o calidad exige que los datos sean, entre otros, comprobables, razón por la cual le corresponde al

21. Cfr. WordReference.com: http://www.wordreference.com/definicion/suplantar
22. Cfr. Parte final del literal a) del artículo 4 (Principio de veracidad o calidad de los registros o datos) de la Ley 1266 de 2008
23. Cfr. Parte final del literal d) del artículo 4 (Principio de veracidad o calidad) de la Ley 1581 de 2012

Responsable demostrar que efectivamente contrató con la persona quien dijo ser y no con un suplantador.

Se desconoce el principio de seguridad porque el suplantador puede incurrir en "consulta, uso o acceso no autorizado o fraudulento"[24] a los datos personales de la persona suplantada, que será el titular del dato afectado. En línea con lo anterior, también se quebranta el principio de circulación restringida porque el suplantador accede a datos personales del titular suplantado sin estar autorizado para ello.[25] En ese sentido, el literal f) del artículo 4 (Principio de acceso y circulación restringida) de la Ley 1581 de 2012 señala que "Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley".

En atención a lo anterior, y con miras a evitar vulneraciones al derecho fundamental de la protección de los datos personales, es crucial que las organizaciones fortalezcan sustancialmente las medidas para establecer la identidad real de las personas en los procesos de contratación, de manera que se pueda comprobar la veracidad de la información sobre su identificación y, al mismo tiempo, impedir situaciones de suplantación de identidad.

Todo proyecto de comercio electrónico debe ir acompañado de procesos y mecanismos confiables que den respuesta, entre otras, a las siguientes preguntas:

i. ¿Cómo tener certeza de que una persona es quien dice ser? (Identidad real de la persona).

ii. Luego de establecida plenamente la identidad de la persona, ¿Cómo identificarla electrónicamente? (identidad virtual o electrónica de la persona).

iii. ¿Cómo impedir suplantaciones físicas o electrónicas de identidad?

iv. ¿Cómo evitar que una persona manifieste que no fue ella quien envió un mensaje de datos o quien expresó su voluntad a través de medios electrónicos?

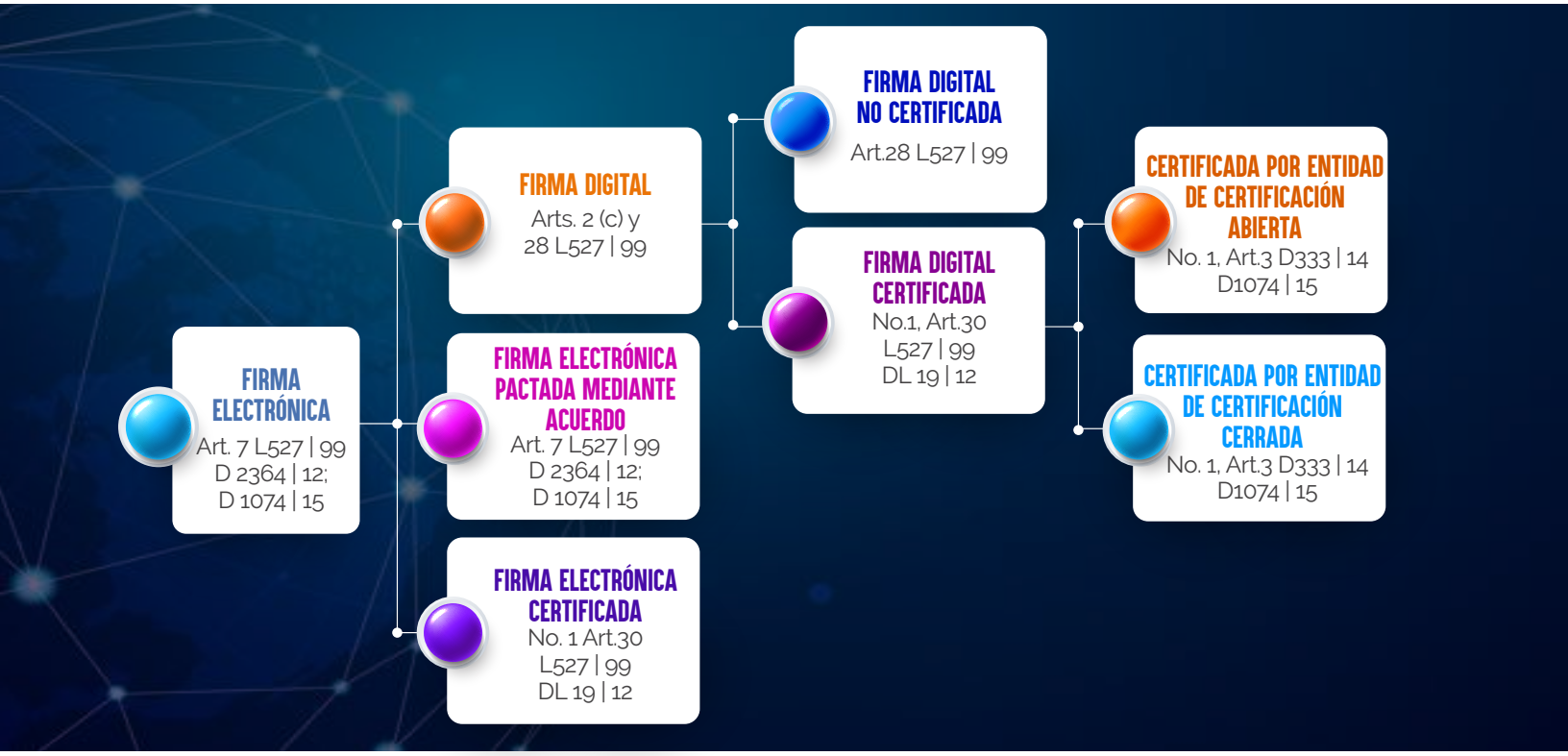
24. Cfr. Literal g) del artículo 4 (Principio de seguridad) de la Ley 1581 de 2012. En este mismo sentido, el literal f) del artículo 4 (Principio de seguridad) de la Ley 1266 de 2008 señala que los datos "se deberán manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su (...) consulta o uso no autorizado".
25. Cfr. Literal c) del artículo 4 (Principio de circulación restringida) de la Ley 1266 de 2008.

Como se observa, establecer la real identidad de quienes participan en el comercio electrónico es uno de los retos que las organizaciones deben asumir. La firma es, entre otros, un método de autenticación y de identificación de las personas. Sobre dicho mecanismo en el contexto electrónico resulta apropiado traer a colación ciertos aspectos de un estudio realizado por la ONU sobre el *"Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas"*[26]

Señala la ONU, entre otros, lo siguiente:

> Los métodos de autenticación y firmas electrónicas pueden clasificarse en tres categorías, a saber: los que se basan en lo que el usuario o el receptor sabe (por ejemplo, contraseñas, números de identificación personal -NIP-), los basados en las características físicas del usuario (por ejemplo, biometría) y los que se fundamentan en la posesión de un objeto por el usuario (por ejemplo, códigos u otra información almacenada en una tarjeta magnética). [...] Entre las tecnologías que se usan en la actualidad figuran las firmas digitales en el marco de una infraestructura de clave pública (ICP), dispositivos biométricos, NIP, contraseñas elegidas por el usuario o asignadas, firmas manuscritas escaneadas, firmas realizadas por medio de un lápiz digital y botones de aceptación de tipo 'sí' o 'aceptar' o 'acepto'. Las soluciones híbridas basadas en la combinación de distintas tecnologías están adquiriendo una aceptación creciente"

En línea con lo señalado por la ONU, la regulación colombiana prevé varias alternativas de identificación electrónica, las cuales sintetizamos en la siguiente gráfica:



26. Organización de las Naciones Unidas (2009). Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas.

La firma electrónica y la firma digital son alternativas de identificación en el contexto digital. La firma electrónica es definida como ***"métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente"***[27] (destacamos). La firma digital, por su parte, es *"**un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación."***[28]

Todas las anteriores opciones de identificación electrónica son jurídicamente válidas, pero su nivel de confiabilidad dependerá del grado de seguridad de:

(1) Los diferentes mecanismos tecnológicos de identificación electrónica que ofrece el mercado.

(2) Los procesos utilizados para identificar a una persona y evitar, por ejemplo, suplantación de identidad.

(3) Las herramientas tecnológicas utilizadas para establecer que esa persona, y no otra, fue quien accedió a la página web y compró un bien.

Así las cosas, según los riesgos de cada proyecto, le corresponde al empresario implementar la alternativa de identificación electrónica más pertinente y segura para establecer la real identidad de las personas y mitigar las situaciones de suplantación de identidad.

VII *Garantizar la seguridad de la información de los consumidores*

El artículo 50 de la ley 1480 de 2011 (Estatuto del Consumidor) señala lo siguiente: "Sin perjuicio de las demás obligaciones establecidas en la presente ley, los proveedores y expendedores ubicados en el territorio nacional que ofrezcan productos utilizando medios electrónicos, deberán: (...) ***f) Adoptar mecanismos de seguridad apropiados y confiables que garanticen la protección de la información personal del consumidor y de la transacción misma. (...)"***

Sin seguridad no habrá un debido Tratamiento de los datos personales. Es fundamental adoptar medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole que eviten:

- *Accesos indebidos o no autorizados a la información.*
- *Manipulación de la información.*
- *Destrucción de la información.*
- *Usos indebidos o no autorización de la información.*
- *Circular o suministrar la información a personas no autorizadas.*

Las medidas de seguridad deben ser apropiadas considerando varios factores como: (i) los niveles de riesgo del Tratamiento para los derechos y libertades de los Titulares de los datos; (ii) la naturaleza de los datos; (iii) las posibles consecuencias que se

27. Cfr. numeral 3 del artículo 1 del Decreto 2364 de 2012.
28. Cfr. literal c del artículo 2 de la Ley 517 de 1999.

derivarían de una vulneración para los Titulares y la magnitud del daño que se puede causar a ellos, al Responsable y a la sociedad en general; (iv) el número de Titulares de los datos y la cantidad de información; (v) el tamaño de la organización; (vi) los recursos disponibles; (vii) el estado de la técnica; y (viii) el alcance, contexto y finalidades del Tratamiento de la información.

Todas las medidas de seguridad deben ser objeto de revisión, evaluación y mejora permanente.

VIII *Verificar que los datos personales fueron obtenidos lícitamente y que pueden ser usados para las actividades que comprende un proyecto de comercio electrónico*

Es crucial tener certeza sobre la legitimación jurídica respecto de la recolección, uso y circulación de los datos personales. Recuerde que está prohibido ***"utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de Datos Personales"*** [29] y que esa actividad debe sujetarse a lo establecido en la ley y las disposiciones que la desarrollen[30]. Adicionalmente, tenga presente que usted debe estar autorizado por el Titular del dato o por la ley para usar la información para fines de comercio electrónico.

Es factible que su empresa adquiera los datos directamente del Titular del dato o que terceros le suministren esa información. En el primer caso, usted debe obtener una autorización previa, expresa e informada que le permita no solo recolectar los datos, sino que también pueda usarlos para fines de comercio electrónico. Es fundamental que la autorización cumpla esos tres requisitos, pues si omite uno de ellos no podrá usar los datos lícitamente. Recuerde que usted no solo debe estar en capacidad de demostrar que tiene prueba de la autorización, también tiene la carga de probar que informó lo que ordena el artículo 12 de la Ley 1581 de 2012.

Tenga presente estos mandatos legales:

- ***"El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento"***[31] (Principio de libertad).
- ***"(...) en el Tratamiento se requiere la autorización***

29. Cfr. Artículo del Decreto 1377 de 2013
30. Cfr. Literal a) del artículo 4 de la Ley 1581 de 2012, el cual se refiere al principio de legalidad en el Tratamiento de Datos Personales

previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior"[32].

• *"El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento"* [33].

• *"Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos"*[34].

• *Es derecho del cliente o de cualquier persona (Titular del dato): "Solicitar prueba de la autorización otorgada al Responsable del Tratamiento"*[35] .

Si su empresa no adquiere los datos directamente de la persona, sino que le son suministrados por terceros, asegúrese de que esos terceros: (i) obtuvieron lícitamente esos datos y (ii) están autorizados a suministrarle a usted esa información para usarla con fines de comercio electrónico. No adquiera bases de datos "piratas", "ilegales" o de dudosa procedencia; ello podría generarle responsabilidad administrativa, civil y penal. En efecto, el delito de violación de datos personales consiste en:

"Artículo 269F: Violación de datos personales. ***El que, sin estar facultado para ello,*** *con provecho propio o de un tercero,* ***obtenga,*** *compile, sustraiga, ofrezca, venda, intercambie, envíe,* ***compre,*** *intercepte, divulgue, modifique o* ***emplee*** *códigos personales,* ***datos personales*** *contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes"*[36]. (Destacamos)

En definitiva, como a la empresa (Responsable del Tratamiento) le corresponde probar que adquirió legítimamente los datos, debe:

IX *Recolectar los datos estrictamente necesarios para fines de comercio electrónico*

Es imperativo tener presente que no se puede recolectar cualquier dato personal, sino solo aquellos que sean imprescindibles para cumplir la finalidad para la cual son colectados. En este sentido, la regulación ordena que ***"la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos"***[37].

31. Cfr. Literal c) del artículo 4 de la Ley 1581 de 2012.
32. Cfr. Artículo 9 de la Ley 1581 de 2012.
33. Cfr. Artículo 5 del Decreto 1377 de 2013.
34. Cfr. Artículo 8 del Decreto 1377 de 2013.
35. Cfr. Literal b) del artículo 8 de la Ley 1581 de 2012
36. Cfr. Artículo 1 de la Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
37. Cfr. Artículo 4 del Decreto 1377 de 2013

X *Dejar de contactar a las personas que no quieren recibir más publicidad y suprimir los datos de contacto cuando lo soliciten*

El uso de los datos no es ilimitado, incondicional, vitalicio o perpetuo. Las personas no están obligadas a recibir publicidad y se debe respetar su decisión en ese sentido cuando ellos se lo comunican.

A pesar de tener autorización de las personas para recolectar y usar su información tenga presente que ellas tienen derecho a revocar su consentimiento y a solicitar la supresión de sus datos personales. Al respecto, la regulación señala:

> ***"Los Titulares podrán en todo momento solicitar al responsable o encargado la supresión de sus datos personales y/o revocar la autorización otorgada para el Tratamiento de los mismos, mediante la presentación de un reclamo, de acuerdo con lo establecido en el artículo 15 de la Ley 1581 de 2012.***
>
> ***La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos.***
>
> ***El responsable y el encargado deben poner a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada"[38].***

Dado lo anterior, es importante que en su organización:

CAPACITE A SU EQUIPO
para que respete y garantice el derecho de las personas de revocar la autorización y suprimir sus datos.

IMPARTA INSTRUCCIONES
para que dejen de llamar o contactar a las personas cuando estas se lo solicitan.

IMPLEMENTE MECANISMOS MANUALES
o automatizados, gratuitos, sencillos y eficaces para que las personas puedan solicitar la supresión de sus datos o la revocatoria de la autorización.

VIGILE Y MONITOREE
si esos mecanismos sirven en la práctica. De no ser así, es factible que el cliente o la persona presente una queja ante la Superintendencia de Industria y Comercio y su empresa pueda ser sancionada hasta por dos mil (2000) salarios mínimos legales mensuales.

MEJORE PERMANENTEMENTE
la atención al cliente, no solo para fortalecer la fidelización y consolidar su confianza, sino para evitar investigaciones y problemas jurídicos.

38. Cfr. Artículo 9 del Decreto 1377 de 2013

XI *Adoptar medidas para garantizar los principios sobre TDP en actividades de comercio electrónico*

Tenga en cuenta que en el desarrollo de las actividades de comercio electrónico se deben aplicar de manera armónica e integral los siguientes principios:

El alcance de cada principio está determinado en el artículo 4 de la Ley 1581 de 2012 y sus normas reglamentarias, razón por la cual nos remitimos al mismo para no transcribirlos en este espacio.

XII *Respetar los derechos de los Titulares de los datos e implementar mecanismos efectivos para el ejercicio de los mismos*

Las organizaciones que desarrollen e implementen proyectos de comercio electrónico deben garantizar los siguientes derechos[39] de los Titulares de los datos:

39. Los derechos están previstos en el artículo 8 de la Ley 1581 de 2012

El alcance de cada derecho está delineado en la Ley 1581 de 2012 y sus decretos reglamentarios, razón por la cual se hace una remisión expresa a dichos textos legales. En todo caso, recuerde que:

- "(L)os procedimientos de acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización deben darse a conocer o ser fácilmente accesibles a los Titulares de la información e incluirse en la política de tratamiento de la información"[39]
- "Los responsables y encargados del tratamiento deben establecer mecanismos sencillos y ágiles que se encuentren permanentemente disponibles a los Titulares con el fin de que estos puedan acceder a los datos personales que estén bajo el control de aquellos y ejercer sus derechos sobre los mismos"[40].
- "Todo Responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente decreto"[41].

XIII *Utilizar herramientas de anonimización*

Es fundamental establecer si es estrictamente necesario que la información que se va a utilizar para proyectos de comercio electrónico debe ir asociada o referirse a una persona. De no ser así, se recomienda que por regla general se utilice información anonimizada de tal manera que no se pueda identificar al Titular del dato.

XIV *Usar los datos de contacto en días y horas que no afecten la tranquilidad de las personas*

Tenga presente que los consumidores pueden sentirse asediados cuando son contactados a través de llamadas telefónicas, mensajes de texto, correos electrónicos y otros medios durante todos los días de la semana y a cualquier hora para fines de prospección comercial.

Dado lo anterior, se recomienda que el uso de los datos personales para actividades de publicidad u ofrecimiento de productos y servicios se realice en días y horarios que no afecten la paz ni la intimidad

39. Cfr. el artículo 18 del Decreto 1377 de 2013
40. Cfr. el artículo 22 del Decreto 1377 de 2013
41. Cfr. el artículo 23 del Decreto 1377 de 2013

familiar, el horario usual de descanso, ni desconozcan su ***"derecho a la tranquilidad"***[42].

Es importante que todo lo anterior esté acompañado de mecanismos de monitoreo y verificación -auditorías internas o externas- con el propósito de asegurar que las medidas implementadas no sólo sean pertinentes, adecuadas o útiles, sino que funcionen correctamente. Adicionalmente, es necesario reforzar las actividades de entrenamiento del equipo de colaboradores para que siempre sean respetuosos y garantistas de los derechos de las personas respecto del tratamiento de sus datos personales.

Es relevante que el autocontrol y la autorregulación formen parte de la política empresarial implementada en las organizaciones para que, por esta vía, se eviten quejas y sanciones.

XV *Incrementar la confianza y la transparencia con sus clientes y terceros Titulares de datos personales*

Desde hace algunas décadas se ha sostenido que la confianza es factor crucial para el crecimiento y consolidación de cualquier actividad que se realice a través del uso de las tecnologías[43]. Lo cual ha sido reiterado al establecer que, ***"las actividades continuas de creación de confianza deben ser una de las prioridades estratégicas más importantes para cada organización"***[44].

"las actividades continuas de creación de confianza deben ser una de las prioridades estratégicas más importantes para cada organización"

"Edelman Trust Barometrer 2019"

42. Cfr. Corte Constitucional, sentencia T-459 de 1998. En este caso la Corte se refiere al derecho a la tranquilidad en los siguientes términos: "Ahora bien, uno de los derechos que deben ser garantizados por el Estado, y que ha ido cobrando importancia dentro de la doctrina constitucional, es el derecho a la tranquilidad, inherente a la persona humana, que le permite al individuo desarrollar una vida digna y sosegada. El derecho a la tranquilidad, lo ha dicho esta Sala, asume el carácter de fundamental por su estrecha relación con la dignidad humana que, necesariamente, conlleva a la paz individual la cual es necesaria para vivir adecuadamente.
(...)

"Como derecho inherente a la persona, el derecho a la tranquilidad debe ser protegido por el Estado de tal forma que permita un ambiente propicio para la convivencia humana, de manera que los individuos puedan realizar sus actividades en un ambiente sano y exento de cualquier molestia que tienda a vulnerar la paz y el sosiego."
43. Cfr. Reichel & Shefter. Harvard Business Review. Jul-Ago, 2000.
44. Cfr. Edelman Trust Barometrer de 2019.https://www.edelman.com/trust-barometer

La confianza se entiende como la expectativa de que "se puede contar con la palabra del otro" y de que se emprenderán acciones positivas y beneficiosas entre las partes de manera recíproca. Cuando existe confianza, la persona cree que la empresa es fiable, cumple su palabra, es sincera, íntegra y lleva a cabo las acciones prometidas[45].

Una organización transparente puede generar mayor confianza en sus clientes y en los Titulares de los datos. Para lograrlo se sugiere lo siguiente:

A

MANTENER CANALES ABIERTOS DE COMUNICACIÓN

y divulgación del uso de los datos personales en los procesos de comercio electrónico. Es importante que esto se haga en términos muy claros y completos, utilizando un lenguaje sencillo que pueda ser entendido por cualquier persona.

B

IMPLEMENTAR UN SISTEMA

efectivo de debida y oportuna atención de quejas y reclamos de los clientes.

C

CUMPLIENDO EN LA PRÁCTICA

lo que se dice o promete en las Políticas de Tratamiento de Información.

45. *Cfr. Barrera Duque, Ernesto (2018) Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales. Universidad de la Sabana y Ecoe ediciones.*

GLOSARIO

Para mayor comprensión de algunos términos utilizados en esta guía, a continuación transcribimos la denominación exacta de cada uno y su definición legal:

AUTORIZACIÓN: *"Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de Datos Personales"*[46].

BASE DE DATOS: *"Conjunto organizado de datos personales que sea objeto de Tratamiento"*[47].

ENCARGADO DEL TRATAMIENTO: *"Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de Datos Personales por cuenta del Responsable del Tratamiento"*[48].

RESPONSABLE DEL TRATAMIENTO: *"Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos"*[49].

TITULAR: *"Persona natural cuyos datos personales sean objeto de Tratamiento"*[50].

TRATAMIENTO: *"Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión"*[51].

DATO PERSONAL: *"Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"*[52].

DATO PRIVADO: *"Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular"*[53].

DATO PÚBLICO: *"Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva"*[54].

DATO SEMIPRIVADO: *"Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley"*[55].

DATOS SENSIBLES: *"Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que prom*ueva

46. Literal a) del artículo 3 de la Ley 1581 de 2012.
47. Literal b) del artículo 3 de la Ley 1581 de 2012.
48. Literal d) del artículo 3 de la Ley 1581 de 2012.
49. Literal e) del artículo 3 de la Ley 1581 de 2012.
50. Literal f) del artículo 3 de la Ley 1581 de 2012.
51. Literal g) del artículo 3 de la Ley 1581 de 2012.
52. Literal c) del artículo 3 de la Ley 1581 de 2012.
53. Literal h) del artículo 3 de la Ley 1266 de 2008.
54. Numeral 2 del artículo 3 del Decreto 1377 de 2013, incorporado en el Decreto Único Reglamentario1074 de 2015.
55. Literal g) del artículo 3 de la Ley 1266 de 2008.

intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos"[56].

TRANSFERENCIA: *"La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de Datos Personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país"*[57].

TRANSMISIÓN: *"Tratamiento de Datos Personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable"*[58].

56. Artículo 5 de la Ley 1581 de 2012 y numeral 3 del artículo 3 del Decreto 1377 de 2013, incorporado en el Decreto Único Reglamentario 1074 de 2015.
57. Numeral 4 del artículo 3 del Decreto 1377 de 2013, incorporado en el Decreto Único Reglamentario1074 de 2015.
58. Numeral 5 del artículo 3 del Decreto 1377 de 2013, incorporado en el Decreto Único Reglamentario1074 de 2015.

DOCUMENTOS CONSULTADOS

Barrera Duque, Ernesto (2018) Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales. Universidad de la Sabana y Ecoe ediciones.

Cavoukia, Ann. Privacidad por Diseño: Los 7 principios fundamentales. Disponible en: http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf

Red Iberoamericana de Protección de Datos (2019). Recomendaciones generales para el Tratamiento de Datos Personales en la Inteligencia Artificial.

OECD (2016), OECD Recommendation of the Council on Consumer Protection in E-Commerce, OECD Publishing, Paris, https://doi.org/10.1787/9789264255258-en.

Organización de las Naciones Unidas (2009). Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas.

Superintendencia de Industria y Comercio (2015) "Guía para implementación del principio de responsabilidad demostrada (accountability)".

Industria y Comercio
SUPERINTENDENCIA

www.sic.gov.co

@sicsuper

Superintendencia de Industria y Comercio de Colombia

Superintendencia de Industria y Comercio

Conmutador: **(571) 5 870 000** - Contact Center: **(571) 5 920 400**
Línea gratuita nacional desde teléfonos fijos: **01 8000 910 165**

El futuro es de todos
Gobierno de Colombia