UNIVERSIDAD EXTERNADO DE COLOMBIA

FACULTAD DE DERECHO

MAESTRÍA EN DERECHO CON ÉNFASIS EN DERECHO INTERNACIONAL DE LOS NEGOCIOS

Rector:	Juan Carlos Henao Pérez
Secretaria General:	Marta Hinestrosa Rey
Decana de la Facultad de Derecho:	Adriana Zapata Giraldo
Directora (e) del Departamento de Derecho de los Negocios:	Adriana Castro Pinzón
Director Trabajo de Grado:	Édgar Iván León Robayo
Jurados:	Daniel Peña Valenzuela Manuel Guerrero Gaitán

CAROLINA HERNÁNDEZ LEÓN

EL PRINCIPIO DE 'ACCOUNTABILITY' EN LA PROTECCIÓN DE DATOS PERSONALES DE LOS CONSUMIDORES DE COMERCIO ELECTRÓNICO

Maestría en Derecho con Énfasis en Derecho Internacional de los Negocios

BOGOTÁ D.C., COLOMBIA

2019

CAROLINA HERNÁNDEZ LEÓN

EL PRINCIPIO DE 'ACCOUNTABILITY' EN LA PROTECCIÓN DE DATOS PERSONALES DE LOS CONSUMIDORES DE COMERCIO ELECTRÓNICO

Trabajo de grado para optar por el título de Magistra en Derecho de los Negocios

Dirigido por:

ÉDGAR IVÁN LEÓN ROBAYO

UNIVERSIDAD EXTERNADO DE COLOMBIA

FACULTAD DE DERECHO

MAESTRÍA EN DERECHO CON ÉNFASIS EN DERECHO INTERNACIONAL DE LOS NEGOCIOS

Bogotá D.C., octubre de 2019

A mis Padres y Hermano por su apoyo incondicional.

AGRADECIMIENTOS

Deseo expresar mi agradecimiento a mi Director de Tesis Édgar Iván León Robayo por su compromiso y apoyo en este proceso realizando valiosas correcciones y sugestiones.

C.H.

ÍNDICE GENERAL

PÁG.

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE CUADROS

ABREVIATURAS

BCR	Binding Corporate Rules
BSC	Balanced Scored Card
CBPR	Cross-Border Privacy Rules
DPA	Autoridades de protección de datos
GDPR	*Reglamento Europeo de Protección de Datos Personales*
IOT	Internet of things
MRGP	Marco de responsabilidad de gestión de privacidad
OCDE	Organización para la Cooperación y el Desarrollo Económicos
PIPEDA	*The Personal Information Protection and Electronic Documents Act*
PMAF	Marco de Responsabilidad de Gestión de Privacidad
RDE	Responsabilidad digital empresarial
RSE	Responsabilidad social empresarial
RIPD	Red Iberoamericana de Protección de Datos

SGSDP	Sistema de gestión de seguridad de datos personales
SIC	Superintendencia de Industria y Comercio
TIC	Tecnologías de la información y la comunicación
UE	Unión Europea

INTRODUCCIÓN

Durante los últimos años, se ha hecho frecuente la utilización de la expresión "Cuarta revolución industrial", para explicar el fenómeno económico con el cual, a través de herramientas digitales, se crean nuevos modelos de negocio que capitalizan la tecnología, creando emprendimientos que abarcan nuevas oportunidades de vivir y trabajar, surgen emprendimientos digitales que se realizan a través de plataformas digitales y consolidan nuevas formas de aprovechar estas herramientas tecnológicas, como es el caso del *Internet of things* (IOT). Estos desarrollos permiten realizar actividades que hasta ahora resultaban insospechadas y que, si bien no solo traen beneficios y ventajas en el estilo de vida de los seres humanos, también se reflejan en lo patrimonial gracias a la creatividad con la que estos instrumentos funcionan.

Este es el caso de empresas como Uber que ideó un modelo de negocio basado en transporte, sin contar con automóviles para ello. O el de Airbnb que inventó un modelo de negocio donde se ofrecen servicios de habitaciones de hotel, sin contar con cuarto o inmueble alguno.

Pero detrás de toda esta actividad existe un aspecto esencial y común que debe ser verificado, controlado, regulado y protegido. Se trata de los derechos que surgen de la recolección y tratamiento de los datos personales de los usuarios de las plataformas digitales, dentro de los cuales se encuentra, fundamentalmente, el derecho de hábeas data. Esta garantía, propia de los Estados democráticos, desarrolla la privacidad de los datos de las personas naturales y permite que los titulares de los datos brinden su consentimiento para la recolección y tratamiento.

Muchas actividades cotidianas requieren la recolección de datos personales. Por ello, las personas naturales bajo su individualidad, y en un ámbito que involucra su privacidad, pueden determinar si permiten la recolección y tratamiento de estos.

Teniendo en cuenta lo anterior, así como el surgimiento de los nuevos modelos de negocio en los que es fundamental la recolección de datos personales de consumidores de comercio electrónico, es importante que las empresas y organizaciones consideren el adecuado tratamiento. Los negocios digitales requieren una estructura de un plan integral de gestión de datos personales que permita que las empresas puedan demostrar un uso adecuado de los datos.

Con el objetivo de poder cumplir con la normativa que existe en relación con la protección de datos personales, se ha vuelto tendencia hacer referencia al principio de *accountability.* Conforme a este postulado se les exige a las empresas demostrar responsabilidad en el cumplimiento de la normativa relacionada con la adecuada protección de datos personales. Además, este principio permite demostrar que las medidas implementadas en una organización son reales y efectivas en la práctica.

Por lo tanto, para lograr una adecuada implementación de este principio en los negocios internacionales y, de esta forma, alcanzar la protección efectiva de los datos personales de los consumidores de comercio electrónico, en una primera parte se determinará en qué consiste y cuál es el contenido del derecho de hábeas data. A continuación, se hará referencia al principio de *accountability* y, finalmente, se estudiarán las medidas jurídicas y tecnológicas que pueden permitir su adecuada implementación en las organizaciones, lo cual permite la efectiva y real protección de los datos personales de los consumidores de comercio electrónico.

CAPÍTULO I
LOS CONSUMIDORES DE COMERCIO ELECTRÓNICO EN LOS NEGOCIOS INTERNACIONALES Y EL DERECHO DE HÁBEAS DATA

Los avances tecnológicos han traído consigo nuevos modelos de negocio, a través de plataformas digitales, que permiten el desarrollo de actividades que se relacionan con los negocios internacionales. De acuerdo con esto, los datos personales de aquellas personas que realizan transacciones a través del comercio electrónico revisten gran importancia dentro de los negocios y para aquellas empresas y organizaciones que los ejecutan.

En este capítulo se hará referencia a las nuevas tecnologías y el acceso que estos nuevos modelos de negocio tienen a mayor cantidad de información personal, que conllevan responsabilidad para las empresas en relación con el manejo que hacen frente a los datos personales. Así mismo, se analizarán algunos instrumentos jurídicos relacionados con la debida protección de datos personales. Adicionalmente, se precisará quién es el consumidor de comercio electrónico.

Por último, se desarrollará el derecho fundamental de hábeas data para lograr una contextualización del mismo en un plano empresarial. El conocimiento de este derecho permitirá estructurar marcos legales que cumplan con los estándares y las regulaciones de los diversos estados en materia de protección de datos personales.

1.1 Sociedad de la información y cuarta revolución industrial

El término sociedad de la información en el mundo occidental fue introducido oficialmente por el sociólogo estadounidense Daniel Bell. El autor afirma que una sociedad posindustrial es básicamente una sociedad de la información. Según su criterio: “El intercambio de

información en términos de varios tipos de procesamiento y almacenamiento de datos, investigación de mercado, etc. (…) es la base de la mayoría de cambios económicos"[1].

La sociedad de la información ha permitido el desarrollo de todo un ecosistema digital. En él los negocios y las actividades comerciales también han percibido cambios, de acuerdo con la tecnología y el surgimiento de la Revolución Industrial 4.0[2].

1.2 Consecuencias del manejo de los datos personales en la era digital

Conforme con los cambios tecnológicos mencionados, las empresas y organizaciones desarrollan hoy en día, además de negocios análogos, transacciones y actividades digitales que permiten llegar a más mercados y a consumidores que hacen uso de las plataformas electrónicas. A su vez, los negocios digitales que se realizan a través de comercio electrónico requieren la recolección, uso y tratamiento de datos personales de clientes y consumidores. Los nuevos negocios tecnológicos han traído, igualmente, cambios en el manejo de los datos. "Estamos en la era de la información y en el mundo de la globalización de los negocios, en donde los datos personales son bienes muy preciados por todos los empresarios"[3].

---

[1] BELL Daniel. The coming of post-industrial society, Basic Books. 1973. Citado por: CRESPI SERRANO Albert y CAÑABATE CARMONA Antonio. ¿Qué es la sociedad de la información? 2010 P. 7.

[2] "La emergente cuarta revolución industrial, es decir, se estaría advirtiendo un gran salto en el proceso de transformación económica, social y tecnológica que se inició en la segunda mitad del siglo XVIII con la llamada primera revolución industrial". —TAPIA, Verónica. Industria 4.0. Internet de las Cosas. UTCIENCIA, [S.l.], v. 1, n. 1, PP 2,3 june 2017. ISSN 2602-8263. Disponible en: http://investigacion.utc.edu.ec/revistasutc/index.php/utciencia/article/view/6/7. Fecha de acceso: 16 de julio de 2019—.

[3] REMOLINA ANGARITA, Nelson. Los datos personales como motor de los negocios. En: Tratamiento de datos personales. Aproximación internacional y comentarios de la Ley 1581 del 2012. Colombia: Editorial Legis, 2013. P. 8.

Al respecto, la *Declaración conjunta sobre comercio electrónico de la Unión Europea y los Estados Unidos* del 5 de diciembre de 1997, afirmó:

> El comercio electrónico ofrece nuevas oportunidades para los negocios y los ciudadanos de todas las regiones del mundo. En particular, las compañías pequeñas podrán conseguir un acceso sin precedentes los mercados mundiales a bajo coste y los consumidores podrán escoger entre un amplio abanico de productos y servicios…[4].

De acuerdo con lo anterior, en un marco empresarial y de negocios surge el comercio electrónico como una de las actividades que hace parte de los negocios internacionales y que permite a las empresas lograr un mayor impacto en el mercado, gracias a la posibilidad de llegar a nuevos consumidores que se encuentran en diversos países del mundo. Esta actividad comercial, que se realiza a través de las tecnologías de la información y la comunicación —en adelante, TIC—permite agregar valor a las operaciones realizadas a través del comercio tradicional, ya que su uso permite realizar:

> Actividades productivas, cuyas operaciones clave, entre ellas las de gestión, financiación, innovación, producción, distribución, ventas y relaciones entre los ocupados y los clientes, tienen lugar en y por internet u otras redes informáticas, sin prejuzgar el grado de conexión entre las dimensiones virtual y física de la empresa[5].

Así, Peña Valenzuela afirma:

> Las tecnologías emergentes crean nuevas oportunidades en los negocios electrónicos. *Blockchain* (cadena de bloques), por ejemplo, aporta al comercio

[4] Declaración conjunta sobre comercio electrónico de la Unión Europea y los Estados Unidos del 5 de diciembre de 1997.

[5] CASTELLS Manuel. La galaxia internet. Barcelona: Areté, 2001, P. 316.

> electrónico la plataforma de pago mediante criptoactivos y también la contratación inteligente que un agregado de las instrucciones del software para ejecutar de manera automatizada instrucciones con la validación de sistemas confiables y descentralizados[6].

Conforme a lo anterior, las cadenas de bloques se convierten entonces en el centro sobre el cual gira todo el sistema, dado que esta nueva tecnología soportada por la tecnología bitcóin, ha logrado consolidar su impacto en diferentes áreas de la sociedad. Estas son definidas por Giménez e Ibáñez como:

> … una base de datos descentralizada, que no puede ser alterada y que se encuentra distribuida entre diferentes participantes, al mismo tiempo que está protegida criptográficamente y organizada en bloques de transacciones relacionados entre ellos de forma matemática[7].

Y agregan:

> La *blockchain* es un libro mayor distribuido que proporciona una manera para que la información sea registrada y compartida por parte de una comunidad. En esta comunidad, cada miembro mantiene su propia copia de la información, y todos los miembros tienen que validar colectivamente cualquier actualización. La información podría representar transacciones, contratos, activos, identidades o prácticamente cualquier cosa que pueda ser descrita de manera digital[8].

---

[6] PEÑA VALENZUELA Daniel. Dos décadas de la Ley de Comercio Electrónico en Colombia [en línea] Bogotá. 22 de julio de 2019.. Disponible en Internet: https://dernegocios.uexternado.edu.co/comercio-electronico/dos-decadas-de-la-ley-de-comercio-electronico-en-colombia/. Fecha de acceso: 22 de julio de 2019]

[7] GIMÉNEZ AUGUST Corrons; IBÁÑEZ Marta Gil. ¿Es la tecnología blockchain compatible con la economía social y solidaria? Hacia un nuevo paradigma. CIRIEC-España, Revista de Economía Pública, Social y Cooperativa, 2019, n.º 95, PP. 191-215 y P. 201.

[8] *Ibid*., P. 202.

De conformidad con lo anterior, tecnologías emergentes como la mencionada aportan al desarrollo de actividades comerciales como el comercio electrónico. De esta forma, las transacciones pueden generar mayor seguridad y confiabilidad tanto para las organizaciones, como para los consumidores.

Este último interviniente en la cadena de comercialización, con los negocios digitales se ha subespecializado y, por ello, es factible hacer referencia actualmente al "consumidor de comercio electrónico", esto es, el adquirente de bienes y servicios a partir de plataformas digitales. Su importancia radica en la necesidad de protección y seguridad que requiere, teniendo en cuenta la relación de desbalance que como cliente tiene frente al empresario que realiza actos de comercio electrónico.

Esta analogía presenta asimetría mayor, teniendo en cuenta que las operaciones de comercio electrónico se realizan a partir de la transferencia de datos informáticos que pueden presentar fallas, lo cual puede desfavorecer al cliente de este tipo de comercio. Según lo indican los consumidores de bienes y servicios son "considerados la "parte débil" del contrato, habida cuenta de la dificultad que tienen para conocer a plenitud lo que se les ofrece en el mercado"[9].

Adicionalmente, se hace necesaria una protección frente a los datos personales de los consumidores de comercio electrónico que los comparten en plataformas digitales o aplicaciones móviles y que requieren información personal para su funcionamiento, donde es ineludible generar confianza y seguridad frente a su tratamiento y uso adecuado.

Para establecer la importancia de gestionar y proteger adecuadamente la información del consumidor de comercio electrónico es fundamental analizar aquellos instrumentos jurídicos internacionales que están relacionados con la protección de datos personales de consumidores de este comercio, determinar quiénes son clientes de esta modalidad de

[9] NAMÉN, J. (2009). La obligación de información en las diferentes fases de la relación del consumo. P. 1.

negocios y cómo se aborda el derecho de hábeas data en un contexto empresarial, lo que permite precisar la importancia para las empresas y los negocios, en la búsqueda de una adecuada gestión de datos personales basado en las buenas prácticas empresariales.

1.3 Principales instrumentos y organizaciones internacionales que han emitido documentos sobre el comercio electrónico y la protección de datos personales

Para lograr un adecuado desarrollo y consolidación de un derecho comercial internacional flexible han surgido iniciativas mundiales por parte de instituciones que buscan fomentar instrumentos que puedan servir a los Estados para poder consolidar su legislación interna en diversas materias. Con el propósito de determinar cuáles son los principales documentos jurídicos relacionados con la protección de datos personales es preciso analizar cuáles organizaciones internacionales se han pronunciado.

1.4 Organismos internacionales que desarrollan temáticas relativas al derecho de hábeas data

En consideración al desarrollo del derecho comercial internacional, se destacan algunos organismos internacionales que han creado agendas temáticas que regulan la protección de datos personales. Uno de ellos es la OCDE la cual ha emitido una serie de documentos relacionados con este tema, dentro de los que se destacan las directrices sobre protección a la privacidad y flujos transfronterizos de datos personales. “Estas directrices aplican a los datos personales del sector público o privado que, debido a la forma en que se procesan, a su naturaleza o al contexto en que se usan, suponen un peligro para la privacidad y las libertades individuales”[10].

A pesar de las recomendaciones que se realizan a los países miembros de esta organización, el alcance de las medidas propuestas allí son medidas de carácter general. Por ello, es

[10] Directrices OCDE sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales. 2002 P. 4.

necesario un esfuerzo por parte de los Estados para desarrollar políticas y leyes internas que permitan una adecuada gestión de la protección de datos personales de los consumidores en las organizaciones. Se necesita tomar medidas que puedan brindar seguridad para los datos e información personal de los consumidores, específicamente aquellos que realizan operaciones a través de comercio electrónico.

Por su parte, las *directrices de la OCDE para la protección de los consumidores de prácticas comerciales transfronterizas fraudulentas y engañosas* recomiendan a los Estados participar en la cooperación y en la búsqueda de mecanismos que permitan evitar que las prácticas comerciales transfronterizas engañosas afecten a los usuarios del comercio electrónico:

> Estas directrices buscan promover la cooperación internacional en contra de las prácticas comerciales fraudulentas y engañosas. Reflejan el compromiso, por parte de los países miembros, para mejorar las leyes y sistemas de aplicación de la ley con el fin de incrementar la efectividad al combatir tales prácticas, al tiempo que reconoce que la cooperación en instancias particulares ocurrirá dentro del marco legal existente. Las directrices se enfocan primordialmente en los órganos públicos nacionales, según lo determine cada país miembro, con autoridad para aplicar las leyes de protección al consumidor[11].

Este documento busca desarrollar principios de cooperación internacional, donde los países miembros y quienes acojan las recomendaciones busquen mejorar las habilidades para combatir estas prácticas comerciales transfronterizas, reconociendo que las agencias tienen la discrecionalidad en la colaboración con la información que puedan suministrar a otras, en las fases de investigación. Así se evidencian esfuerzos, por parte de la OCDE, para consolidar recomendaciones que puedan servir a los Estados en materia de protección al

[11] MÉXICO. PROCURADURÍA FEDERAL DEL CONSUMIDOR (PROFECO), México Publicado en acuerdo con la OCDE, París. Directrices de la OCDE para la protección de los consumidores de prácticas comerciales transfronterizas fraudulentas y engañosas. 2004. Consultado: 7 de septiembre de 2019. P. 11.

consumidor en materia de posibles prácticas fraudulentas o engañosas que puedan realizarse a través de comercio electrónico.

Además, existen otros instrumentos internacionales en materia de protección de datos personales tales como los *Estándares de protección de datos personales para los estados Iberoamericanos* (2017). Esta herramienta contiene directrices que buscan orientar a los países de la región iberoamericana que no cuentan con ordenamientos jurídicos relacionados con la protección de datos personales, además de ser un referente para poder modernizar y actualizar las legislaciones que actualmente existen.

Dentro de su objeto se observa:

> (i) establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región, (ii) garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales, (iii) facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región …[12].

Adicionalmente, la Organización de Estados Americanos —en adelante, OEA— ha emitido los *Principios de la OEA sobre privacidad y protección de datos personales con anotaciones* (2015), cuyo objetivo es crear un marco jurídico de protección de datos personales y la autodeterminación relacionada con la información personal. En relación con la protección de datos personales de consumidores de comercio electrónico, este documento precisa:

[12] RED IBEROAMERICANA DE PROTECCIÓN DE DATOS. Estándares de Protección de Datos Personales para los Estados Iberoamericanos. 20 de junio de 2017. P. 7.

> Las normas relativas a la privacidad deben permitir que los consumidores y las empresas se beneficien del uso de datos personales de una manera segura y protegida. Deben ser equilibradas y tecnológicamente neutrales y permitir el libre flujo de datos dentro de cada país y a través de fronteras nacionales de una manera que fomente la innovación tecnológica y promueva el desarrollo económico y el crecimiento del comercio".

Como se aprecia, este instrumento jurídico menciona la protección de datos relacionada con los actos de comercio electrónico, en concordancia con el principio de neutralidad tecnológica:

> La aplicación analógica del derecho cuando la actividad realizada es exactamente la misma independientemente del soporte utilizado, lo que supone implícitamente la existencia de límites en la aplicación de normas vigentes para actividades novedosas y, asimismo, por la concepción social del nuevo ámbito de interacción social que es internet[13].

Adicionalmente, se observa una mención al principio de equivalencia funcional, el cual:

> … procura que la información en forma de mensaje de datos tenga reconocimiento jurídico en similares términos a sus homólogos del comercio tradicional. En esas circunstancias, los efectos jurídicos de los actos realizados por medios electrónicos serán iguales a los realizados por otros cauces[14].

[13] ESPINOSA ALONSO Carles. La información en la red y el principio de neutralidad tecnológica: la libertad de expresión y la difusión de información administrativa. En: *Revista Vasca de Administración Pública n.º 81*,2009 P. 87.

[14] POLANCO LÓPEZ Hugo Armando. Manifestaciones del principio de equivalencia funcional y no discriminación en el ordenamiento jurídico colombiano. Revista Criterio Jurídico. Santiago de Cali 2016 ISSN 1657-3978 P. 43.

Si bien los instrumentos jurídicos internacionales mencionados evidencian referencias a la temática que se investiga. Sin embargo, teniendo en cuenta la importancia de la información personal, relacionada con el derecho de hábeas data en un contexto de desarrollo de negocios, a través de comercio electrónico, es necesario profundizar en su análisis y en los aportes que puedan realizar a las legislaciones de diversos países, así como las organizaciones internacionales en esta materia.

1.5 El consumidor de comercio electrónico en los negocios internacionales

Gran parte del desarrollo económico y la evolución de los negocios internacionales giran en torno a las actividades como el comercio electrónico. Por ello,

> El consumidor es el sujeto fundamental en la relación jurídica por medios electrónicos. Su protección específica derivada del reconocimiento de su debilidad por la ausencia del contratante en este tipo de contratación ha sido el fundamento de la regulación legal del comercio electrónico. Podría decirse que el 'derecho del comercio electrónico' surge precisamente como una respuesta a la necesidad de mayor confianza en las actividades en la red[15].

A continuación, se explicará el concepto de consumidor de comercio electrónico, término que surge como una nueva categoría de usuario, teniendo en cuenta su comportamiento frente a las plataformas mediante las cuales se realizan los negocios digitales en la actualidad.

1.5.1 El consumidor de comercio electrónico

La tecnología ha incentivado cambios que se han visto reflejados en las conductas de los consumidores de comercio electrónico. Teniendo en cuenta el desarrollo de los negocios

[15] PEÑA VALENZUELA Daniel. Tecnologías de la información y derecho del consumo-tendencias y perplejidades. En: Contexto. Revista de Derecho y Economía n.º 19 (2004) p. 1.

digitales, en este tipo de transacciones, los clientes pueden llegar a ser más vulnerables dada la intangibilidad de estas; además, en materia de publicidad, por ejemplo, la creación de necesidades en un ámbito virtual en ocasiones pueden no corresponder con necesidades reales.

> Es evidente entonces que el consumidor se enfrenta a varios riesgos producto de la asimetría informativa en cuanto al objeto de la prestación y la asimetría tecnológica, pues han surgido nuevas tecnologías de *marketing*, lo que se acentúa en el caso de Internet, que permite hacer publicidad dentro del hogar del consumidor[16].

Al respecto, Lorenzetti afirma:

> Este principio de protección al consumidor evolucionó desde las reglas clásicas dentro del derecho obligacional, como la de protección al deudor (*favor debitoris*), asumiendo que este es la parte débil en las relaciones jurídicas, a la de *favor debilis* que pretende proteger al *débil* en la relación jurídica, dependiendo del grupo de contratos y contratantes específicos, tales como los trabajadores, arrendatarios o locatarios, etc.[17].

Como se aprecia, la desigualdad en la relación que existe entre el proveedor y el consumidor de comercio electrónico es una realidad. Por lo tanto, surge la necesidad de brindar una protección real y efectiva para el cliente de comercio electrónico en relación con las operaciones que se derivan de la realización de este tipo de negocios.

---

[16] RODRÍGUEZ Gladys Stella. Riesgos del consumidor de comercio electrónico en las prácticas publicitarias. Revista de Derecho n.º 37, Barranquilla, 2012. ISSN: 0121- 869 P. 268. Disponible en [PDF].

[17] OVIEDO ALBÁN Jorge. Consumidores. (PDF) En: Dikaíon -Lo Justo-Noviembre de 2006, Año 20 n.º 15 - Chía-Colombia P. 483. Consultado el 18 de julio de 2019.

1.5.2 Protección requerida por el consumidor

Ahora, es importante mencionar, que la protección jurídica requerida por el consumidor puede verse desde dos ópticas: la primera se encuentra relacionada con las garantías necesarias para la buena ejecución del contrato electrónico. Al respecto Peña Valenzuela afirma:

> Los esquemas de comercio electrónico en redes abiertas requieren de ambas partes, productor y consumidor, un grado de confianza en la validez de los contratos electrónicos. A diferencia de los contratos tradicionales en los que prima la autonomía privada y el consentimiento, en los contratos electrónicos las categorías principales son los términos y condiciones de uso de portales así como las licencias de uso con el consentimiento por navegación, sin mayor expresión del consentimiento[18].

La segunda perspectiva se refiere al tratamiento de la información personal de los consumidores de comercio electrónico. Este punto se relaciona directamente con el uso y la gestión de los datos que son recabados por distintas organizaciones y que necesitan una adecuada protección. Este asunto se encuentra ligado con el derecho de hábeas data que busca la efectiva protección de los datos e información personal.

Es importante decir, además, que la asimetría informativa en un contexto digital, no solo se evidencia en relación, por ejemplo, con la publicidad que llega a los consumidores a través de internet. También se puede manifestar en la forma como las empresas que realizan negocios de comercio electrónico recolectan información personal de consumidores y materializan el tratamiento de esta, bien sea para el uso que le darán en su negocio propio o frente a la información personal que pueden compartir frente a terceros, como consecuencia de las diferentes operaciones o actividades que pueden hacer. Por lo tanto, es importante

[18] PEÑA VALENZUELA Daniel. Tecnologías de la información y derecho del consumo-tendencias y perplejidades. Op. cit. P. 62.

que las empresas determinen sistemas adecuados de recolección y tratamiento de datos personales, con el fin de minimizar el desbalance que puede haber entre ellas como proveedores de comercio electrónico y los clientes.

En las transacciones en red, el consumidor busca seguridad y confiabilidad frente a las operaciones que realiza y, además, requiere que la información personal se gestione adecuadamente. En la era de la información actual, la información personal y los datos se consolidan como activos que requieren adecuada gestión y manejo por parte de terceros.

> El concepto de 'aldea global' acuñado por el sociólogo canadiense Marshall Mcluhan cobra más fuerza que nunca. Las formas en que accedemos a la información, nos conectamos e interactuamos con otros han abierto un nuevo espacio para todos, un espacio que se ha convertido en una extensión de nuestro cuerpo, entre lo presencial y lo digital[19].

Seguidamente se abordará el análisis del derecho de hábeas data, conforme al desarrollo en un contexto empresarial y de negocios.

1.6 El derecho de hábeas data en el contexto de negocios que se realizan a través de comercio electrónico

Para contextualizar el derecho de hábeas data es importante definirlo, para luego poder analizar su manifestación en relación con la protección de datos personales en un contexto empresarial, de esta forma, es posible comprender el marco legal general del tratamiento de datos personales y cuáles son las implicaciones en relación con las empresas u organizaciones que hacen recolección y tratamiento de estos.

[19] CASTAÑO PELÁEZ Adrián. ¿Qué es la revolución digital? En: *Nueva Sociedad. Revista latinoamericana de ciencias sociales*. (2016).

Gracias a los nuevos modelos de negocio *on-line*, los empresarios que realizan negocios de comercio electrónico desarrollan tratamiento de datos personales de clientes y consumidores. Esta es una exigencia que plantean los nuevos esquemas de modelos de negocio. Como consecuencia, es importante determinar la magnitud que puede llegar alcanzar este tratamiento de datos personales, teniendo en cuenta la importancia de su protección:

> Buscar la protección efectiva de la privacidad se sitúa como un componente importante para considerar a una sociedad como democrática. Se trata de un derecho fundamental. Este derecho fundamental se materializa en la posibilidad de las personas naturales de dirigir su información personal. La intimidad se convierte en una pieza primordial de la autodeterminación en la sociedad del conocimiento[20].

La existencia y consolidación de una sociedad democrática tienen como punto de partida el respeto y la garantía de los derechos humanos y las libertades. Por esto, "resulta trascendental no dejar de mencionar, así sea someramente, que la protección de datos es considerada como un elemento consustancial de la democracia"[21].

1.6.1 El derecho de hábeas data

Este derecho es considerado como fundamental, goza de rango constitucional y se encuentra regulado por los Estados. Desde la perspectiva de los negocios digitales, podemos decir que:

[20] BRUNET NAHABETIÁN Laura. Protección de datos y gestión documental: Decálogo ampliado para la sociedad de la información. Rev.Fac.Der n.º 39 Montevideo July 2015. Versión en línea: ISSN 2301-0665 P. 204.

[21] *Ibid*., P. 205.

> (…) vivimos en un mundo global e hiperconectado, pero con diferencias sociales, culturales, económicas y legales en cada país. Pese a ello, se ha procurado lograr un consenso *internacional* sobre el contenido mínimo de los textos que regulan el tratamiento de datos personales y las instituciones para hacer cumplir esos mínimos y exigir un debido tratamiento de la información en estudio. No existe unanimidad sobre todas las cuestiones, razón por la cual coexisten diferentes enfoques de protección (…)[22].

Aunque no existe concordancia en un único sistema que regule la protección de datos personales a nivel mundial, existen al menos cinco alternativas de *regulación* para proteger los datos personales y otros derechos conexos, a saber: disposiciones constitucionales, leyes generales, leyes sectoriales, la contratación y la autorregulación[23].

> Cada país define el camino [que se va] a tomar para abordar este tema. En algunos casos se recurre a una mixtura complementaria de estos modelos para garantizar un nivel mínimo de protección a los ciudadanos frente al tratamiento de sus datos personales. Es el caso, por ejemplo, de Colombia, donde existen normas constitucionales, normas generales y sectoriales junto con contratos y normas corporativas vinculantes[24].

1.6.2 Regulación en Colombia del derecho de hábeas data

El sistema mixto colombiano parte de la base de una regulación constitucional en el artículo 15 de la Constitución Política que indica:

---

[22] REMOLINA ANGARITA Nelson, Los datos personales como motor de los negocios. En: Tratamiento de datos personales. Aproximación internacional y comentarios de la Ley 1581 del 2012. Colombia. Editorial Legis, 2013. Op. cit. P. 16.

[23] *Ibid*., P. 16.

[24] *Ibid*., P. 16.

> Todas las personas tienen derecho a su intimidad personal y familiar a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas[25].

Adicionalmente, existen normas que regulan y desarrollan el derecho fundamental de hábeas data, es el caso de la Ley 1581 del 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales"[26] y el Decreto Reglamentario 1377 del 2013: "Por el cual se reglamenta parcialmente la Ley 1581 de 2012"[27]. Estas normativas deben ser cumplidas por personas naturales o jurídicas que realicen tratamiento de datos personales.

Existe otra preceptiva relacionada con la protección de datos de consumidores en Colombia que se encuentra relacionada con los negocios que se realizan a través de plataformas de comercio electrónico. Se trata de la Ley 1480 del 2011 (Estatuto del Consumidor), Al respecto, se manifiesta:

> La efectividad de los derechos del consumidor dependerá de: (i) la labor que realicen las autoridades competentes, (ii) la postura ética y el compromiso social de las empresas y (iii) el rol del consumidor, siendo más cuidadoso y diligente a la hora de comprar utilizando las TIC para dicho efecto[28].

---

[25] Colombia. Artículo 15 Constitución Política de Colombia.

[26] COLOMBIA. Congreso de la República. Diario Oficial 48.587 de 18 de octubre de 2012. Ley Estatutaria 1581 del 2012 [En línea] [Consultado el: 23 de julio de 2019] Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[27] COLOMBIA. Ministerio de Comercio, Industria y Turismo. Decreto 1377 del 2013.

[28] REMOLINA ANGARITA Nelson. La protección del consumidor en el comercio electrónico. https://www.ambitojuridico.com/noticias/columnista-impreso/mercantil-propiedad-intelectual-y-arbitraje/la-proteccion-del. Fecha de acceso: 11 de febrero de 2019.

1.6.3 Hábeas data en contexto internacional

En un plano internacional, si se analiza este tema se encuentra que el sistema norteamericano "(…) no considera la protección de datos como un derecho fundamental, sino como un derecho del consumidor"[29]. Por su parte, el europeo considera que el hábeas data es un derecho fundamental y, por lo tanto, requiere una fuerte regulación y protección, dado que "concibe la protección de datos como un derecho fundamental"[30].

Ahora bien, en un ámbito empresarial, donde los negocios se han digitalizado y se realizan a través de plataformas de comercio electrónico, los modelos de negocios en internet, en múltiples ocasiones, requieren el uso de datos personales de consumidores de comercio electrónico:

> Las tecnologías de la información y la comunicación (TIC), por su parte, han contribuido a la *datificación* de la sociedad contemporánea y a la consolidación del dato personal como el bien más apetecido de la economía digital. Esto obedece a muchas razones pero, principalmente, a que los datos personales son la moneda de la economía digital o la moneda de oro del siglo XXI[31].

Al respecto, Barrera Duque menciona:

---

[29] REMOLINA ANGARITA Nelson. Tratamiento de datos personales. Aproximación internacional y comentarios de la Ley 1581 del 2012, Op. cit. P. 19.

[30] *Ibid*., P. 19.

[31] REMOLINA ANGARITA Nelson. ÁLVAREZ ZULUAGA, Luisa Fernanda. (2018). Guía GECTI para la implementación del principio de responsabilidad demostrada –*accountability*– en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos. Universidad de los Andes (Bogotá, Colombia). Facultad de Derecho. GECTI, 1-58. p. 10.

> Nos preocupamos por el *data protection* en la medida en que los nuevos modelos *on-line* implican la utilización de información privada de los clientes con miras a segmentar y personalizar la oferta de servicios y productos[32].

De acuerdo con lo anterior, conforme al avance de la tecnología y el surgimiento de nuevos modelos de negocio, este tipo de plataformas requieren el uso de información personal de clientes y consumidores de comercio electrónico. Es un deber de las organizaciones hacer un buen uso de los datos que le han sido suministrados.

Al obtener conocimiento acerca del derecho de hábeas data es posible crear esquemas que determinen la mejor manera de custodiar adecuadamente la información. Comprender que se encuentra ligado con la intimidad y la esfera personal permite adoptar las mejores medidas para lograr proteger adecuadamente dicha información y ofrecer seguridad al consumidor de comercio electrónico.

1.7 Conclusiones del capítulo

Los nuevos modelos de negocios en ecosistemas digitales han permitido a las empresas y a las organizaciones expandir los negocios y llegar a nuevos consumidores que requieren servicios o productos en diferentes países del mundo. Conforme al desarrollo de esta clase de negocios es necesaria la recolección y tratamiento de datos personales, lo cual se constituye en un elemento importante para el funcionamiento de las plataformas de comercio electrónico.

Existen diversos sistemas e instrumentos jurídicos que han desarrollado esta temática, donde se evidencia una responsabilidad, por parte de las empresas que realizan recolección y tratamiento de datos personales, para el funcionamiento de sus modelos orgánicos de

[32] BARRERA DUQUE Ernesto. “Modelos de negocios en Internet”, en: Internet, Comercio Electrónico & Telecomunicaciones, Bogotá. GECTI, Universidad de los Andes, Editorial Legis, 2002, PP. 216-217.

negocio *on-line*. Sin embargo, aunque plantean la importancia de una adecuada gestión de datos personales en las organizaciones, estos documentos no responden del todo a los desafíos que impone la tecnología y a los esquemas que revisten este tipo de negocios.

Al analizar el derecho de hábeas data, es fundamental conocer en qué consiste y cuál es su manifestación de acuerdo con los sistemas regulatorios de datos personales a escala mundial. De esta forma, se podrá determinar la importancia en un contexto empresarial y, a partir de aquí, los empresarios tendrán oportunidad de crear estrategias y políticas que permitan cumplir con la debida custodia de los datos de los consumidores de comercio electrónico.

Uno de los desafíos más importantes en esta materia consiste en transferir este conocimiento. De esta manera, se podrán crear sistemas de gestión de datos que respondan a estos retos y que demuestren en la práctica un trabajo conjunto entre los gerentes de las empresas y los operadores empresariales, con el fin de lograr una adecuada gestión de datos personales que brinde seguridad y confiabilidad a los consumidores de comercio electrónico.

En el siguiente capítulo se abordará el principio de *accountability*, sus elementos y los beneficios que puede otorgar a los empresarios al momento de estructurarlo e implementarlo en una organización.

CAPÍTULO II
PRINCIPIO DE 'ACCOUNTABILITY' EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Actualmente, las empresas que realizan actividades comerciales y negocios a través de comercio electrónico, requieren almacenar y dar tratamiento a la información de tipo personal y confidencial. Esta recolección de información personal se relaciona con aquellos consumidores que hacen uso de las plataformas de comercio electrónico que estas empresas manejan. La base de este tipo de negocios requiere información personal para su funcionamiento, esto se evidencia cuando la recolección de datos se realiza con fines publicitarios y de creación de bases de datos que regulen tendencias en los consumidores, entre otros aspectos importantes para este tipo de empresas y negocios.

Teniendo en cuenta la relevancia que tienen los datos personales, hoy en día, es vital que las empresas y organizaciones consideren un tratamiento adecuado y gestión de los datos que almacenan, ya que un buen uso y proceso de datos personales puede garantizar el efectivo cumplimiento y respeto del derecho de hábeas data.

> La protección de la intimidad frente a la informática no significa impedir el proceso electrónico de informaciones, necesarias en el funcionamiento de cualquier Estado moderno, sino el aseguramiento de un uso democrático de la *Information Technology*[33].

[33] PÉREZ LUÑO Antonio Enrique. Derechos humanos (...), cit., nota 19, P. 345. Citado por: GARCÍA GONZÁLEZ Aristeo. La protección de datos personales: Derecho Fundamental del Siglo XXI. Un Estudio Comparado. Boletín Mexicano de Derecho Comparado, nueva serie, año XL, núm. 120, septiembre-diciembre de 2007, P. 751.

A partir de este punto, se hace necesario crear marcos legales empresariales que garanticen buenas prácticas en materia de gestión y protección de datos personales de los consumidores de comercio electrónico. Con respecto a la protección de datos y la vida privada, Consumers International plantea:

> Los datos personales son valiosos para las empresas en línea porque enriquecen su conocimiento del mercado y les permiten establecer un perfil de cada consumidor. Los problemas que se plantean en relación con la protección de la vida privada y los datos son, entre otros, el desconocimiento de cómo se utilizan en Internet los datos recopilados, la determinación de responsabilidades en caso de violación de la confidencialidad de los datos, la transmisión de datos a terceros y la determinación del derecho aplicable y la jurisdicción competente[34].

Para precisar en qué consiste el principio de *accountability*, es vital analizar su definición y elementos, además de los beneficios que puede ofrecer a las organizaciones frente a la prospección de crear mecanismos adecuados de protección de datos personales para los consumidores de comercio electrónico. Además, es necesario considerar su escenario internacional, ya que países como Canadá, Hong Kong y Colombia han contemplado este principio en sus legislaciones y lo han relacionado con la protección adecuada de los datos personales y las buenas prácticas.

2.1 El principio de 'accountability'

Según Remolina:

> El término *accountability* (responsabilidad) proviene del mundo anglosajón y a pesar de las diferentes acepciones que puedan darse de él, se ha entendido que

[34] CONSUMIDORES INTERNACIONALES. Citado por: Naciones Unidas. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. Protección de los consumidores en el comercio electrónico. 2017. p. 10.

> en la arena de la protección de datos dicha expresión se refiere al modo como una organización debe cumplir en la práctica las regulaciones sobre la materia y a la manera como debe demostrar que lo hecho es útil, pertinente y eficiente[35].

Este principio ha sido mencionado y reconocido por varios instrumentos jurídicos. Así:

> Las directrices OCDE de 1980 sobre Protección a la Privacidad y Flujos Transfronterizos de datos personales es uno de ellos y fue el primer documento con implicaciones de tipo internacional en materia de protección de datos y privacidad[36].

La OCDE realizó una actualización de estas directrices en el año 2013, donde incluyó la definición de esta forma:

> Apartado 14: Principio de la responsabilidad 62. El controlador de datos decide sobre los datos y las actividades de proceso de datos. El proceso de datos se realiza en su beneficio. Así pues, es fundamental que la ley local le exija al controlador la responsabilidad de cumplir con las normas y decisiones sobre la protección de la privacidad; y el hecho de que el proceso de datos lo realice otra persona, como una oficina de servicios, en su nombre, no debería bastar para que el controlador de datos quedará libre de esta obligación (…)[37].

---

[35] REMOLINA ANGARITA Nelson. ÁLVAREZ ZULUAGA Luisa Fernanda. (2018). Guía GECTI para la implementación del principio de responsabilidad demostrada —*accountability*— en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos. Op. cit. pp. 28-29.

[36] GETTING ACCOUNTABILITY RIGHT WITH A PRIVACY MANAGEMENT PROGRAM. P. 3. Disponible en: https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf. Fecha de acceso: 28 de septiembre de 2019. Materiales preparados por las oficinas del Comisionado de Privacidad de Canadá y el Comisionado de Privacidad e Información de British Columbia. Traducido por la autora.

[37] DIRECTRICES OCDE DE 1980 SOBRE PROTECCIÓN A LA PRIVACIDAD Y FLUJOS TRANSFRONTERIZOS DE DATOS PERSONALES. 2004, Organisation for Economic Cooperation and

Por su parte, el Comisionado de Privacidad de Canadá (OPC) y las oficinas de los comisionados de la información y la privacidad (OIPC) de Alberta y British Columbia, lo definen así:

> En relación con la privacidad se trata de la aceptación de la responsabilidad para la debida protección de la información personal. Una organización responsable debe tener en su lugar políticas y procedimientos que promuevan las buenas prácticas, las cuales se deben tomar como un todo y constituyen un programa de gestión de privacidad. El resultado es una capacidad demostrable de cumplimiento, como mínimo, con las leyes de privacidad aplicables[38].

Igualmente, en el documento: *Cómo permitir la protección efectiva de datos y la confianza en la sociedad digital* elaborado por el Centre for Information Policy Leadership[39], el principio es conceptualizado de la siguiente forma:

> La responsabilidad ahora tiene un amplio apoyo internacional y ha sido adoptada en muchas leyes, incluso en el Reglamento General de Protección de Datos (GDPR) de la UE, las políticas regulatorias y las prácticas organizativas. Es esencial que exista consenso y claridad sobre el significado preciso y la aplicación de la responsabilidad de la organización entre todas las partes

---

Development (OECD), París. y Ministerio de Administraciones Públicas, Secretaría General Técnica, España P. 21 Disponible en [PDF].

[38] *Ibid*., P 1. Disponible en: https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf. Fecha de acceso: 28 de septiembre de 2019.

[39] Grupo de expertos de privacidad y seguridad global con sede en Washington, D.C., Bruselas y Londres. CIPL que trabaja con líderes de la industria, autoridades reguladoras y formuladores de políticas para desarrollar soluciones globales y mejores prácticas para la privacidad y el uso responsable de los datos para permitir la era de la información moderna —Centre For Information Policy Leadership. Who we are. Disponible en: https://www.informationpolicycentre.com/about.html—.

> interesadas, incluidas las organizaciones que implementan la responsabilidad y las DPA que supervisan la responsabilidad[40].

La Unión Europea también ha demostrado interés en esta materia. Aunque no existe una directiva que regule directamente este tema, este organismo de integración ha manifestado:

> La opinión del grupo de trabajo del artículo 29 sobre responsabilidad contiene un análisis detallado de lo que significa la rendición de cuentas en la privacidad y lo que se podría esperar de las organizaciones en el futuro para demostrar el cumplimiento, y presenta una propuesta que considera que debería ayudar a práctica, así como ayudar a las autoridades de protección de datos en sus tareas de supervisión y cumplimiento[41].

En Colombia, el principio de *accountability* ha sido incorporado al ordenamiento jurídico en el artículo 26 del Decreto 1377 del 2013 en el artículo 26:

> Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 del 2012 y este decreto, en una manera que sea proporcional a lo siguiente: 1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente. 2. La naturaleza de los datos personales objeto del

[40] The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, Centre for Information Policy Leadership 23 de julio de 2018. Disponible en: [PDF] P. 3.

[41] Getting Accountability Right with a Privacy Management Program. Op. cit., P. 4.

> tratamiento. 3. El tipo de tratamiento. 4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares[42].

Como vemos, la importancia del principio de *accountability* radica en la necesidad de proteger favorablemente la información o datos personales, por parte de las empresas u organizaciones, para lograr el efectivo cumplimiento del derecho de hábeas data. Por lo tanto, instituciones internacionales se han encargado de estudiar y analizar este principio como ocurre con la "The Information Accountability Foundation", entidad que se ha encargado de analizar y documentar información relativa a este principio. Dentro de sus principales objetivos están:

> Promover la gobernanza de la información basada en la rendición de cuentas a través de consultas e investigaciones activas, en colaboración con los gobiernos, los organismos de aplicación, las empresas y la sociedad civil, por lo que la protección de datos puede ser eficaz para facilitar la innovación impulsada por la información y proteger los derechos de las personas a la privacidad y la autonomía[43].

Esta entidad trabaja en conjunto con las entidades reguladoras, empresarios, aquellos encargados de formular políticas relacionadas con la adecuada protección de datos personales y la sociedad civil[44]. Por ello, su objetivo:

---

[42] PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 1377 de 2013. Artículo 26. Disponible en PDF.

[43] Perfil de Linkedin: The Information Accountability Foundation. Disponible en Internet: https://co.linkedin.com/company/the-information-accountability-foundation. Fecha de acceso: 28 de septiembre de 2019.

[44] THE INFORMATION ACCOUNTABILITY FOUNDATION. Disponible en: http://informationaccountability.org/. Fecha de acceso: 8 de septiembre de 2019.

> (…) a través de consultas e investigaciones activas, es lograr sistemas efectivos de gobernanza de la información para facilitar la innovación impulsada por la información y al mismo tiempo proteger los derechos de las personas a la privacidad y la autonomía[45].

2.2 Elementos del principio de 'accountability'

El principio de *accountability* conlleva obligaciones por parte de empresas y organizaciones que realizan el tratamiento de datos personales. Por un lado, es necesario que logren demostrar el grado de responsabilidad en relación con el fin para el cual realizan recolección y tratamiento de datos personales y, por el otro, las entidades deben demostrar que sus programas internos de gestión y manejo de datos personales, cumplen con los estándares requeridos por ley tanto nacional, como aquellas disposiciones y estándares internacionales.

Los elementos que hacen parte del principio de *accountability*, y de los cuales se tratará a continuación, han sido analizados y estudiados por diversas organizaciones internacionales que trabajan temas de protección de datos personales. Dentro de estas instituciones podemos encontrar: The Centre for Information Policy Leadership Hunton & Williams LLP, Centre for Information Policy Leadership, The Information Accountability Foundation, entre otras. En relación con este tema, se han logrado consensos en relación con el análisis de los elementos comunes al principio de *accountability*.

> El diálogo global sobre responsabilidad creó y adoptó los elementos esenciales de la rendición de cuentas en el 2009. Este marco describe los elementos del programa de lo que un administrador responsable de los datos tendría para ser responsable. Esos elementos esenciales se han institucionalizado en la

[45] *Ibid*. THE INFORMATION ACCOUNTABILITY FOUNDATION. Foundation Mission.

> orientación del regulador y las nuevas leyes de protección de datos. Las organizaciones las han incorporado en sus políticas y procedimientos[46].

Después de varios debates en relación con los elementos esenciales que debe abarcar el principio de *accountability*, se determinaron lineamientos acerca de las medidas que deben tomar las organizaciones para lograr una adecuada implementación del principio.

> En abril del 2009, se inició un diálogo global para proporcionar orientación sobre cómo las organizaciones podrían demostrar su uso responsable y la gestión de la información personal. Los participantes incluyeron representantes de la industria, el gobierno, la sociedad civil, el mundo académico y las empresas que se reunieron para discutir los elementos de la rendición de cuentas con perspectivas de Europa, América del Norte y la región Asia-Pacífico[47].

De acuerdo con The Centre for Information Policy Leadership Hunton & Williams LLP que ha trabajado en el proyecto *Accountability* dividido en tres fases, la primera fase se trata del proyecto Galway que trabaja los elementos de este principio:

> Una organización responsable demuestra compromiso con la responsabilidad, implementa políticas de privacidad de datos vinculadas a criterios externos reconocidos y establece el desempeño y mecanismos para asegurar la toma

[46] ABRAMS Martin; ABRAMS John; CULLEN Peter.; GOLDSTEIN Lynn. Apéndice. "Enhanced Accountability Elements for Artificial Intelligence (AI) and Machine Learning that Directly Impacts People" The Information Accountability Foundation: Artificial Intelligence, Ethics and Enhanced Data Stewardship. 20 de septiembre de 2017. P. 18. Traducido por la autora.

[47] THE INFORMATION ACCOUNTABILITY FOUNDATION: The Global Information Accountability Project: The First Five Years. 22 de mayo de 2014. P. 4. Traducido por la autora.

> responsable de decisiones sobre la gestión de datos consistente con las políticas de la organización[48].

Conforme a lo anterior, el documento que reguló el proyecto Galway reunió a una serie de expertos que buscaron enfocar el principio de *accountability* hacia un sistema de gobernanza global de datos, donde se analizó el desarrollo del principio que puede abordarse desde dos perspectivas: una nacional, en la cual los Estados tienen sus regulaciones propias, y una internacional donde existen regulaciones que determinan estándares de cumplimiento frente a la protección de datos personales. Al respecto, en este proyecto se concluyó:

> Hacer realidad la rendición de cuentas requiere que las empresas apliquen esos conceptos para que su gestión de la información sea segura y productiva. Nuestras conversaciones sugirieron además que la creciente complejidad de los datos, la recopilación y el uso requieren que gran parte de la carga para protegerlos deba pasar del individuo a la organización[49].

La tercera fase del proyecto *Accountability* realizó estudios y análisis para determinar los elementos del principio. Para lograr su cometido, fueron partícipes de los debates y discusiones con respecto a este tema, expertos en materias regulatorias relacionadas con la debida protección de datos personales. Más adelante, se describirán y detallarán estos elementos que son de vital importancia para las organizaciones al momento de estructurar programas de gestión integral de datos personales.

---

[48] THE CENTRE FOR INFORMATION POLICY LEADERSHIP HUNTON & WILLIAMS LLP. Accountability: A Compendium for Stakeholders. Marzo de 2011. Data Protection Accountability: The Essential Elements. A Document for Discussion October 2009. Prepared by the Centre for Information Policy Leadership as Secretariat to the Galway Project. p 1. Traducido por la autora.

[49] *Ibid* ., P. 3.

2.2.1 Compromiso de la organización para implementar el principio de 'accountability' y adopción de políticas internas

De acuerdo con el Centre for Information Policy Leadership:

> Una organización debe demostrar su voluntad y capacidad para ser ambos comprometidos y responsables de sus prácticas de datos. Una organización debe implementar políticas vinculadas a criterios externos apropiados (que se encuentran en la ley, principios generalmente aceptados o las mejores prácticas de la industria) y diseñado para proporcionar al individuo una protección de privacidad efectiva, desplegar mecanismos para actuar en relación con esas políticas y monitorear esos mecanismos[50].

Para poder crear marcos legales que permitan gestionar *accountability* en una organización es necesario primero que las entidades determinen la importancia y relevancia que tiene este principio y a partir de aquí puedan crear políticas y estrategias internas que les permitan llegar al desarrollo de buenas prácticas en materia de datos personales.

2.2.2 Mecanismos para poner en práctica las políticas de privacidad, incluyendo herramientas, capacitación y educación

Es vital que las organizaciones puedan contar con un marco legal que logre implementar las políticas y directrices que estén relacionadas con el principio de *accountability*, por ello:

> La organización debe establecer mecanismos de desempeño para implementar políticas de privacidad establecidas. Los mecanismos podrían incluir herramientas para facilitar la toma de decisiones sobre el uso y la protección adecuados de los datos, capacitación sobre cómo utilizar esas herramientas y

[50] *Idem*, P. 11. Traducido por la autora.

> procesos para asegurar el cumplimiento de los empleados que recolectan, procesan y protegen información. Las herramientas y la capacitación deben ser obligatorios para aquellos individuos clave involucrados en la recolección y despliegue de información personal[51].

Adicionalmente, una organización debe contar con los medios adecuados para la aplicar los métodos y medidas necesarios para llevar a cabo dichas regulaciones. Para lograr esto, es primordial considerar a los trabajadores como parte significativa de este proceso. Esto se puede materializar a través de la capacitación para los operadores, donde se explique claramente la relevancia que tiene la información personal. De esta forma, se puede crear cultura empresarial de buenas prácticas en materia de datos personales, donde participan en conjunto empresa y trabajadores para poder alcanzar los fines que persigue el desarrollo de este principio.

2.2.3 Sistemas para revisiones internas continuas y opiniones de garantía y verificación externa

Mediante el análisis de gestión de riesgos, las empresas que recolectan y utilizan información personal

> (…) deben monitorear y medir si las políticas que han adoptado e implementado, protegen y aseguran los datos. Las organizaciones responsables establecen estos sistemas de monitoreo de desempeño. Basados en sus propias culturas empresariales[52].

Para establecer los marcos legales que gestionen adecuadamente los datos personales de clientes y consumidores es necesario establecer programas que logren asegurar aquellas políticas y estrategias que la empresa u organización han establecido. Además, es

[51] *Idem*, p 12

[52] *Idem*.

importante determinar sistemas de monitoreo continuo y eficaz, que logren demostrar que aquellas políticas y estrategias encaminadas a la protección adecuada de los datos funcionan y ofrecen niveles adecuados de garantía para los consumidores.

2.2.4 Transparencia y mecanismos de protección individual

La transparencia frente a los procesos mediante los cuales la organización va a realizar el tratamiento de datos es fundamental en relación con el consumidor. Esto crea seguridad y confiabilidad respecto de este usuario. Es así como

> Para facilitar la participación individual, los procedimientos de la organización deben ser transparentes. La articulación de los procedimientos de información de la organización y las protecciones en un aviso de privacidad publicado, siguen siendo clave para el compromiso individual. La organización responsable desarrolla una estrategia para realizar comunicación prominente a las personas acerca de la información más importante[53].

En este punto, es importante decir que las organizaciones tienen la responsabilidad de encontrar medios eficaces y transparentes para informar a los titulares de datos personales acerca de cuál o cuáles van a ser los usos que su información va a tener con respecto a esta organización. Esta transparencia puede manifestarse a través de mecanismos que permitan recolectar adecuadamente la información. En este punto podemos mencionar medios como formularios de contacto, avisos de privacidad, íconos, entre otros.

2.2.5. Medios para subsanar y aplicación externa

Es fundamental que las organizaciones cuenten con medios que permitan abordar adecuadamente los daños o perjuicios que se puedan ocasionar a los consumidores con

[53] *Idem*, P 13.

ocasión de las fallas que se encuentren relacionadas con las políticas de privacidad y los sistemas de *compliance* internos y propios de la organización

> Una organización responsable también puede contratar un servicio de subsanación externo para solucionar problemas que puedan surgir con los consumidores como las quejas y reclamos. Los auditores externos y los programas de sellos de certificación y servicios de resolución de disputas, pueden facilitar la interacción entre el consumidor y la organización, de esta forma podría mejorar su reputación para cumplir con las políticas y obligaciones con las personas naturales[54].

También, es relevante que, al momento de producirse una falla dentro de los sistemas internos de gestión de datos existan mecanismos o recursos para que los consumidores de comercio electrónico puedan hacer valer sus derechos. Además, es vital poder contar también con terceros que puedan aportar en la resolución de quejas de los clientes acerca del manejo de datos personales.

Teniendo en cuenta el surgimiento de negocios digitales que conllevan actividades como el comercio electrónico, entre otros aspectos, The Information Accountability Foundation (IAF) desarrolló el documento "Enhanced Data Stewardship Accountability Elements" que determinó una mejora en los elementos determinados por el proyecto Galway que desarrolló los elementos del principio de *accountability*. Al respecto, esta fundación indicó que:

> Para ser capaz de transformar los datos en información y la información en conocimiento y visión, y a su vez el conocimiento en ventaja competitiva, para que los individuos puedan confiar en las actividades de procesamiento de datos

[54] *Idem*, P 14.

que podrían no estar dentro de sus expectativas, se necesita una mejor responsabilidad de la administración de datos (responsabilidad mejorada)[55].

Al transformar los datos en información es importante que las organizaciones determinen el alcance de su responsabilidad, lo cual puede generar ventajas de tipo competitivo, teniendo en cuenta la seguridad y confiabilidad que pueden obtener por parte de los consumidores y, a su vez, crear fidelización, gracias a la seguridad que ofrece una empresa al hacer uso adecuado de los datos personales de los consumidores.

Lograr implementar los elementos de la responsabilidad demostrada sirve de ayuda en el camino para estructurar e implementar el principio; sin embargo, las mejoras que estos elementos han tenido conforme al avance de la tecnología, puede ayudar a una mejor implementación, cumpliendo con una responsabilidad demostrada por parte de las organizaciones.

Adicionalmente, la comunidad de organizaciones que ha estudiado y analizado los temas más importantes de la protección de datos personales ha comenzado a tratar el principio de *accountability* 2.0, relacionado con los negocios que se realizan actualmente en las plataformas digitales.

2.3 Beneficios del principio de 'accountability'

El principio de *accountability* permite lograr esquemas adecuados de protección de datos personales, esto va alineado con diversos aspectos que deben tener en cuenta las organizaciones, para poder obtener los mejores resultados en cuanto a su desarrollo e implementación. Esta responsabilidad conlleva deberes para las empresas y organizaciones al momento de poder demostrar que aquellas medidas y estrategias que fueron tomadas en la organización, producen efectos en la práctica. La medición de la real eficacia y eficiencia

[55] The Information Accountability Foundation. Data Stewardship Elements. January 2019. p 2.

de las estrategias que han sido tomadas por una organización se da en relación con la evaluación de resultados que pueda demostrar efectivamente. Esto es válido si las estrategias que fueron tomadas para aplicar el principio de *accountability* se desarrollan en la práctica.

Los beneficios que puede ofrecer un adecuado desarrollo e implementación del principio de *accountability*, en las organizaciones, está orientado a las herramientas que este axioma puede brindar. Al respecto, The Information Accountability Foundation ha agrupado los beneficios que conlleva una adecuada implementación del principio de responsabilidad demostrada, de acuerdo con los beneficios que pueden favorecer a los grupos o partes de interés, como lo son las organizaciones, los individuos o personas naturales y los Estados, conforme se tratará a continuación[56]:

2.3.1 Beneficios para las organizaciones

Al momento de implementar las políticas que se ajusten a los marcos regulatorios de protección de datos personales se pueden evitar vulneraciones a los derechos de los consumidores, así como fugas de datos que pongan en riesgo la información personal de los clientes y amenazas internas que puedan crear vulnerabilidades en los esquemas de custodia de datos.

Dentro de los beneficios más destacables en esta materia para las organizaciones se pueden encontrar: protección de la privacidad de manera más efectiva, por cuanto se requiere de una priorización basada en el riesgo. En efecto, al delimitar cuáles son los posibles riesgos que se pueden derivar del manejo y tratamiento de datos personales es posible encontrar mecanismos de mitigación de los mismos y tomar medidas más efectivas en torno a la privacidad y al debido cuidado de los datos personales de los individuos. El principio de

[56] Centre for Information Policy Leadership. The Central Role of Organizational Accountability in Data Protection. The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society. Op., cit. pp. 19 y 20. Traducido por la autora.

accountability permite determinar los riesgos frente al tratamiento de dicha información y, de esta forma, priorizar las medidas tendientes a minimizarlos.

Además, las organizaciones pueden involucrarse en usos más beneficiosos de los datos personales, donde se incluyen aspectos como la investigación y la inteligencia artificial responsable y el aprendizaje automático, al minimizar los riesgos de los nuevos usos de datos por ejemplo, mediante la incorporación de privacidad por diseño, transparencia, evaluación de riesgos, etc. y demostrar el uso responsable de los datos a los reguladores.

Dentro de los beneficios que se pueden contemplar a partir de la puesta en marcha de los aspectos básicos del principio de *accountability*, encontramos la posibilidad mediante la cual las organizaciones pueden obtener un uso y conocimiento de datos personales importantes, teniendo en cuenta variables como tecnología, investigación y el bien social, entre otros aspectos. En este punto, es fundamental mencionar que el concepto de evaluación de riesgos permite determinar las posibles amenazas frente a las cuales pueden verse expuestos los datos personales de clientes y consumidores. De esta forma, es posible tomar medidas adecuadas que logren mitigar esos peligros.

Además, es preciso brindar seguridad jurídica a las organizaciones con respecto al cumplimiento de la protección de datos, a través de las fronteras, por medio de la participación en marcos de responsabilidad reconocidos como BCR y CBPR. Estos últimos constituyen normas de carácter vinculante conforme al Reglamento Europeo de Protección de Datos Personales (GDPR). De acuerdo con esta preceptiva, las normas BCR son:

> (…) políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países

> terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta[57].

De acuerdo con lo anterior, es importante que las organizaciones puedan determinar esquemas regulatorios adecuados conforme a las normas corporativas vinculantes BCR y CBPR que, aunque son normas aplicables para la Unión Europea, también lo son para aquellas empresas que realicen recolección y tratamiento de datos personales de ciudadanos europeos. Esto implica que las empresas y organizaciones deben tener conocimiento acerca del reglamento GDPR y las normas que contiene. De esta manera, se pueden evitar transgresiones a la legislación de datos personales europea.

Promover la creación de interoperabilidad entre diferentes marcos de responsabilidad y, por lo tanto, de soluciones globales para la transferencia de datos para las organizaciones, una de las problemáticas que surge en torno al desarrollo de negocios digitales, se encuentra relacionada con las transferencias de datos. Muchos de ellos deben ser compartidos entre varias organizaciones, teniendo en cuenta el modelo de negocio que manejan las empresas. Como consecuencia, la privacidad de las personas naturales podría verse afectada. Por lo tanto, es absolutamente necesario que las organizaciones promuevan sistemas cooperativos que permitan generar colaboración entre Estados para poder tener un mejor seguimiento en relación con el uso de la información personal de clientes y consumidores de comercio electrónico y, de esta forma, lograr una efectiva protección del derecho de hábeas data. Más aún, cuando están de por medio mecanismos como la transferencia internacional de datos.

2.3.2 Beneficios para las personas naturales

Igualmente, los individuos encuentran en el principio de *accountability* una serie de ventajas en relación con la protección de los datos personales, como pueden ser las siguientes:

[57] Unión Europea. Reglamento GDPR, artículo 4º, apartado 20.

> Garantiza el cumplimiento de los requisitos legales locales y aumenta la confianza que tienen las personas en el procesamiento de sus datos por parte de las organizaciones. La importancia de crear tranquilidad en relación con el uso de los datos personales puede ser determinante frente a la confianza en la empresa y el interés de continuar adquiriendo productos y servicios frente a una sensación de confianza que determina el uso correcto de los datos personales, teniendo en cuenta que estos hacen parte de la intimidad de los sujetos.

Como se aprecia, es factible una aplicación interna y transfronteriza de datos más efectiva. Crear estándares de aplicación del principio de *accountability* en las organizaciones permite tener un mayor y mejor control en la recolección, el tratamiento de datos y su transferencia internacional, a escala nacional e internacional. En efecto, estas tienen una responsabilidad adicional, teniendo en cuenta factores como, por ejemplo, la facilitación tecnológica actual del intercambio de bases de datos, lo que les genera retos frente a la protección y privacidad de los clientes y consumidores. De ello debe haber constante información veraz y oportuna, de manera que estos puedan determinar finalmente si están de acuerdo con entregar su información.

2.3.3 Tipos y categorías de beneficios del principio de 'accountability'

Al momento de su implementación en las empresas u organizaciones, se puede evidenciar la obtención de múltiples beneficios tanto para los socios como para los inversionistas. Como primera medida, es importante crear marcos legales que cumplan con estándares de responsabilidad demostrada y cuya armonización permita alcanzar objetivos en diferentes jurisdicciones. La creación de programas integrales de gestión de protección de datos personales puede servir de base para cumplir con las distintas normativas tanto nacionales como internacionales:

> El programa interno de privacidad de una organización multinacional, basado en los elementos de responsabilidad demostrada, permite alinear las políticas y

> prácticas de privacidad con los diversos requisitos de las diferentes jurisdicciones en las que opera y armonizarlas (sic) tanto como sea posible. El programa interno de privacidad de la organización, en efecto, crea un puente práctico entre diferentes requisitos legales[58].

La estructuración de marcos legales y programas internos que regulen el principio de *accountability* se debe basar en los elementos primordiales que desarrollan este principio, para lograr enfilar sus objetivos con las legislaciones donde tienen su domicilio y, de esta manera, lograr concordancia y mayor y mejor adopción de los requerimientos de los diversos Estados donde pueden tener domicilio sus sucursales o filiales. Estos programas garantizan que las medidas que una organización ha tomado en relación con la gestión y el tratamiento de datos personales cumplen y demuestran eficacia y eficiencia en su implementación.

> Implementar un programa basado en la rendición de cuentas, ya sea certificado o no, es una herramienta poderosa para que las organizaciones garanticen y demuestren que cumplen con la legislación nacional aplicable (o, en la UE, el GDPR)[59].

Como se aprecia, la configuración de marcos legales y programas que demuestren el cumplimiento del principio de *accountability* permite garantizar que las organizaciones cumplen con las legislaciones nacionales y con legislaciones, como aquella aplicable a la UE a través del reglamento GDPR, que regula las temáticas relacionadas con la protección de datos personales y que exige, entre otras cosas, que esta normativa sea aplicable a aquellas empresas que realizan recolección y tratamiento de datos personales de los ciudadanos europeos. Al respecto, el reglamento establece:

---

[58] *Idem,* p 21.

[59] *Idem,* P. 22.

> El tratamiento de datos personales de los interesados que residen en la Unión por un responsable o encargado no establecido en la Unión debe ser también objeto del presente reglamento cuando esté relacionado con la observación del comportamiento de dichos interesados en la medida en que este comportamiento tenga lugar en la Unión[60].

Del mismo modo, el principio de *accountability* también puede utilizarse como herramienta de la debida diligencia para obtener ventajas competitivas en el mercado. Cuando las organizaciones logran estructurar planes integrales de gestión de datos personales, consiguen demostrar responsabilidad acerca de las buenas prácticas que deben tener al momento de hacer su recolección y tratamiento. Esta responsabilidad no solo se manifiesta frente a los consumidores, pues también es posible que su cumplimiento se pueda demostrar ante posibles socios, lo cual puede ser una ventaja en los mercados.

> Este beneficio de la rendición de cuentas se basa en el hecho de que los esquemas basados en el principio de *accountability* requieren una infraestructura de cumplimiento interna verificada, que incluye políticas escritas y otra documentación, que permiten a la organización demostrar su responsabilidad y cumplimiento no solo ante los reguladores sino ante posibles socios comerciales[61].

Igualmente, el desarrollo de esquemas y marcos legales que incluyan el principio de responsabilidad demostrada permite les permite a las organizaciones cumplir con los estándares requeridos para un buen manejo de datos personales de los clientes y consumidores. Lo anterior, tanto de empresas que realizan negocios análogos, como de empresas que realizan negocios digitales a través de comercio electrónico.

---

[60] Unión Europea. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016. p 5.

[61] *Idem*, p 23.

Por otro lado, es preciso considerar al principio de *accountability* como facilitador de confianza en relación con los nuevos modelos digitales que requieren uso de datos personales para su adecuado funcionamiento. La tecnología ha generado un gran procesamiento de datos que se genera en internet o, incluso, la nube. Como consecuencia, el sistema maneja grandes cantidades de datos e información que en ocasiones se encuentra por fuera del conocimiento de las personas naturales.

> Esto es especialmente cierto en los últimos años con el auge de las redes sociales, el *big data*, los dispositivos de Internet de las cosas y la inteligencia artificial. Estas tecnologías crearon un cambio fundamental en la generación y recopilación de datos personales y, junto con los cambios en las dinámicas y comportamientos organizativos y de los consumidores[62].

El principio de *accountability* impone cargas para las organizaciones en relación con la debida protección de los datos personales de consumidores. Cuando estas instituciones cumplen con los estándares derivados del principio y establecen métricas que les permitan evaluar el impacto de dichas estrategias y políticas pueden generarles confianza a sus clientes acerca del uso que se le da a su información personal.

De acuerdo con lo anteriormente expuesto, es fundamental conocer en qué consiste este principio y cuáles son los elementos para lograr implementarlo en un esquema de buenas prácticas empresariales en materia de protección de datos de la organización. En el contexto de derecho preventivo, que busca mitigar y minimizar riesgos de tipo jurídico, es importante determinar un documento organizacional que regule la implementación de este principio y que garantice el adecuado cumplimiento de tales directrices.

Del mismo modo, de acuerdo con los nuevos esquemas empresariales, que son orgánicos y variables de manera que permitan alcanzar mejoras organizacionales, resulta fundamental

[62] *Idem*, p 24.

generar mecanismos internos de auditoría en relación con el manejo y gestión de los datos personales. De esta forma, se crean instrumentos internos de verificación de *compliance* (cumplimiento) que pueden determinar si las políticas y directrices de la organización se cumplen.

Así, el principio de *accountability* se constituye en una herramienta fundamental para el desarrollo de esquemas y marcos legales que cumplan con los estándares relacionados con la debida y adecuada protección de datos personales, los cuales se resumen en la Tabla 1.

Tabla 1

Beneficios del principio de 'accountability'

Organizacionales	Protección de datos de los consumidores con base en los análisis de riesgos que permiten determinar las posibles amenazas o vulneraciones frente a los datos personales
Individuales	Gestionar esquemas adecuados de protección de datos personales crea seguridad y confiabilidad en el consumidor de comercio electrónico
Compliance interno	Crear planes de gestión integral de datos personales permite que las organizaciones actúen de acuerdo con la normativa y los estándares para el desarrollo de buenas prácticas empresariales en materia de protección de datos personales.

Fuente: Autoría propia.

2.4 Conclusiones del capítulo

Las empresas y organizaciones deben conocer en qué consiste el principio de *accountability*. De esta forma resulta posible implementar este postulado como herramienta auxiliar al momento de crear y estructurar nuevos planes integrales de gestión de datos personales. Existen múltiples beneficios para una organización al momento de implementar

el principio en los marcos legales y regulatorios de buenas prácticas. La confianza en el consumidor acerca del manejo que se les da a sus datos personales se puede traducir en fidelidad hacia la empresa y cumple con la confiabilidad y seguridad que genera para los clientes.

En relación con otras empresas o negocios, una adecuada implementación del principio de *accountability* puede generar confianza en las relaciones comerciales. Además, lograr una medición de la eficacia de los programas, también se consolida como un elemento mediante el cual las empresas pueden demostrar que están cumpliendo a cabalidad con la normativa que la ley y los estándares internacionales les exigen para un debido tratamiento de datos personales.

En el próximo capítulo se desarrollará el principio de *accountability* en la práctica y las herramientas a través de las cuales se puede lograr su adecuada implementación.

CAPÍTULO III
LA EFECTIVA PROTECCIÓN DEL CONSUMIDOR DE COMERCIO ELECTRÓNICO BAJO EL PRINCIPIO DE 'ACCOUNTABILITY'

Las nuevas tecnologías derivadas del desarrollo de la cuarta revolución industrial[63] facilitan de una mejor manera la globalización de los negocios y la posibilidad de las empresas y organizaciones de llegar a nuevos consumidores. Esto logra una expansión de los negocios y la posibilidad de impactar nuevos mercados que permitan generar mayores utilidades.

A partir de los nuevos esquemas de actividades comerciales electrónicas, como ocurre por ejemplo con las plataformas digitales[64], surgen modelos de negocios innovadores que funcionan a través de ecosistemas digitales y que exigen la recolección, uso y tratamiento de datos personales por parte de las empresas y organizaciones.

De esta forma, las empresas que realizan negocios digitales tienen la obligación de realizar una adecuada recolección, manejo y gestión de los datos de sus clientes o consumidores. Parte del auge que reviste actualmente el tema de protección de datos a escala mundial es precisamente la coyuntura de escándalos como el de Facebook-Analytica, que develó fallas profundas en los sistemas de manejo y gestión de datos.

---

[63] De acuerdo con GRAEME Codrington, en su video: "The best explanation of the Fourth Industrial Revolution ever", la cuarta revolución industrial es la aplicación de la tecnología a nuestro mundo, que otorga la oportunidad de cambiar la forma de vivir y trabajar. Cuestiona los nuevos negocios y emprendimientos para preguntar: ¿Hay alguna otra forma de hacer las cosas? Video disponible en: https://youtu.be/okXk4Bnz2Lc. Fecha de acceso: 20 de septiembre de 2019.

[64] Según GRAEME existen organizaciones en esta cuarta revolución industrial que han logrado revolucionar los negocios. Ejemplos como Uber, que se trata de una empresa de taxis sin carros o Airbnb que es un hotel sin habitaciones, nuevos modelos de negocio digitales que responden a una nueva forma de trabajar, utilizando herramientas digitales que permiten hacer cosas nuevas que no se han realizado antes. *Ibid*.

> En una era de sobrecarga de datos, de flujos inesperados de información, se hace cada vez más relevante hacer conciencia de la importancia del tratamiento de la información. Así como muchas organizaciones hoy trabajan para ser 'socialmente responsables', estatus que le brinda oportunidades y visibilidad en los mercados, aumentando su reputación, de igual forma deben comenzar a trabajar para ser "digitalmente responsables[65].

Es fundamental considerar entonces el valor que representan los datos para las empresas y organizaciones. De aquí, se deriva una responsabilidad social digital que, de acuerdo con lo indicado por Cooper, Siu y Wei:

> Las empresas que tendrán éxito en esta nueva y desafiante economía digital, serán aquellas que desarrollen una "responsabilidad digital empresarial", una responsabilidad que se traduce en una incorporación plena y trascendente del tratamiento adecuado de la información[66].

Adicionalmente, los autores explican que las empresas deben adoptar la doctrina emergente de la "responsabilidad digital corporativa" para facilitar la navegación de manera efectiva en "el ámbito de datos y dispositivos en constante expansión"[67].

De acuerdo con lo anterior, en el flujo transfronterizo de los datos, consecuencia de los negocios digitales, existe una responsabilidad digital corporativa para las organizaciones que hacen recolección y tratamiento de datos personales. Para determinar su alcance es

[65] CANO MARTÍNEZ, Jeimy. 2016. ¿Eres una empresa digitalmente responsable? Enero 20. [En línea] Disponible en: https://www.linkedin.com/pulse/eres-una-empresa-digitalmente-responsable-jeimycano-ph-d-cfe. Fecha de acceso: 28 de septiembre de 2019.

[66] COOPER Tim, SIU Jade, WEI Kuangy. Corporate Digital Responsibility. Doing well by doing good. Citado por: CANO MARTÍNEZ Jeimy. ¿Eres una empresa digitalmente responsable? 2016.

[67] COOPER Tim, SIU Jade, WEI Kuangy. Corporate Digital Responsibility. Doing well by doing good [PDF] En: Outlook The on-line journal of high-performance business. p 3. Fecha de acceso: 28 de septiembre de 2019.

importante conocer el desarrollo del principio de *accountability* en la práctica. Esto es, algunos casos que revelan deficiencias en los esquemas que gestionan los datos personales a nivel interno en una empresa u organización y la adecuada implementación basada en tecnología del mencionado postulado, con el fin de aplicar los métodos y las medidas necesarias para gestionar adecuadamente este principio y proteger la información personal de los consumidores de comercio electrónico.

Conforme a lo anterior, es fundamental determinar los mecanismos mediante los cuales se puede implementar el principio de *accountability* en las organizaciones para lograr una debida gestión y protección de los datos personales de los clientes y consumidores de comercio electrónico. De esta forma, se cumplen preceptos de derecho preventivo que buscan mitigar riesgos de tipo jurídico en las empresas y que a su vez buscan implementar correctamente los requerimientos legales en materia de protección de datos personales. Todo esto encaminado a evitar multas, sanciones económicas y procesos tediosos que conllevan pérdida de dinero y tiempo para las empresas y que, adicionalmente, pueden representar un impacto negativo también en cuanto a su reputación en el mercado.

3.1 Desarrollo del principio de 'accountability' en la práctica

El desarrollo del principio de *accountability* se basa principalmente en los esquemas empresariales que buscan la consolidación de buenas prácticas corporativas en relación con una adecuada protección de datos personales. Con el fin de lograr una consolidación que permita su implementación efectiva y eficaz en las organizaciones que realizan negocios internacionales, a través de comercio electrónico, es importante que las empresas consideren crear guías internas y marcos legales documentales, o basados en sistemas de información, haciendo uso de la tecnología y que busquen gestionar los aspectos básicos de este principio.

> En materia de responsabilidad demostrada o demostrable no basta hacer, sino probar lo que se hizo. Aunque existe libertad de utilizar diversos mecanismos

> probatorios, tenga presente que las normas de protección de datos imponen cargas probatorias que usted debe estar en capacidad de acreditar plenamente[68].

Por lo tanto, es necesario crear una serie de documentos internos en la organización o marcos legales regulatorios apoyados en la tecnología, que logren demostrar efectivamente que existen medidas en relación con el desarrollo del principio de *accountability*. Es fundamental que las organizaciones creen marcos legales regulatorios y autorregulatorios que abarquen su desarrollo y que les permita lograr correlativamente una implementación que conceda llevar estas medidas y estrategias internas que pueden encontrarse en una guía regulatoria a la práctica. De esta forma, es posible probar que las medidas que se tomaron para la regulación de este principio, están surtiendo efectos en la praxis, lo cual demuestra una completa y eficaz implementación.

Adicionalmente, es necesario crear programas integrales de gestión de datos personales que logren demostrar tanto la implementación adecuada de los estándares normativos, como la eficacia real en la práctica, que permita medir efectivamente que la información de los consumidores de comercio electrónico se encuentra debidamente protegida.

3.1.1 Guías internacionales que regulan la protección de datos personales

En relación con el desarrollo del principio de *accountability*, diversas legislaciones en el mundo han dado a conocer y puesto en vigencia documentos y guías que pueden servir de orientación para las organizaciones y empresas que realizan negocios digitales. Según se hizo referencia en el capítulo anterior, en Colombia es la Dirección de Investigación de Protección de Datos Personales de la SIC, la entidad que ejerce:

[68] REMOLINA Álvarez. Guía GECTI para la implementación del principio de responsabilidad demostrada —*accountability*— en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos. Op. cit., p 38.

> (…) la vigilancia de los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países de la misma naturaleza, en cuanto se refiere a la actividad de administración de datos personales[69].

Es así como en desarrollo de esta función en el año 2016 expidió la *Guía para la implementación del principio de responsabilidad demostrada (accountability)*: "Este documento responde al llamado de la industria que ha solicitado mayor orientación en el camino de construir un Programa Integral de Gestión de Datos Personales"[70].

Y en otro aparte, indicó:

> En el caso colombiano: El ordenamiento jurídico colombiano exige que los sujetos obligados adopten políticas internas efectivas, por disposición expresa del artículo 27 del Decreto 1377 del 2013. Estas políticas internas efectivas no pueden limitarse a reproducir los textos legales ni son meras declaraciones de principios. Por el contrario, la adopción de políticas internas efectivas parte del desarrollo de un Programa Integral de Gestión de Datos Personales, que debe ser el resultado de un proceso de debida diligencia en la organización que permita formularlo[71].

Además, en relación con la efectiva evidencia de una adecuada implementación del principio de *accountability*, la SIC indicó:

---

[69] Superintendencia de Industria y Comercio. Objetivos y funciones [en línea]. Disponible en Internet: http://www.sic.gov.co/objetivos-y-funciones. Fecha de acceso: 12 de agosto de 2019.

[70] Superintendencia de Industria y Comercio. Guía para la Implementación del Principio de Responsabilidad Demostrada (*accountability*). [PDF] 2016. P 4.

[71] *Ibid*., p 8.

> La regulación colombiana le impone al responsable o al encargado del tratamiento la responsabilidad de garantizar la eficacia de los derechos del titular del dato, la cual no puede ser simbólica ni formal, sino real y demostrable[72].

Conforme a lo expuesto por el organismo de vigilancia y control, las medidas que deben ser tomadas por las empresas y organizaciones deben demostrar su efectividad[73]. En este sentido, la Red Iberoamericana de Protección de Datos (RIPD), ha indicado:

> La autorregulación solo redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales[74].

[72] COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 83882 de 2018. [PDF] Por la cual se resuelve un recurso de apelación. Bogotá D.C., 2018. P 14 Disponible en Internet en: http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/Resolucion83882de2018.pdf. Fecha de acceso: 19 de agosto de 2019.

[73] "Corresponde al responsable o al encargado probar que ha puesto en marcha las medidas adecuadas, útiles y eficaces para cumplir la regulación.", COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 83882 de 2018. p 15.

[74] Red Iberoamericana de Protección de Datos. Grupo de Trabajo temporal sobre autorregulación y protección de datos personales. Mayo 5 de 2006. Citado por: COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 83882 de 2018. p 16.

Por otro lado, a escala internacional se encuentran ejemplos como el de Canadá. La Oficina del Comisionado de Privacidad de ese país ha emitido también una guía para aquellas organizaciones sometidas a Pipeda. Esta ley determina que las organizaciones deben cumplir con requerimientos en relación con las políticas de tratamiento de datos personales, entre los aspectos más relevantes se encuentra: (i) obtener el consentimiento del titular al momento de la recolección de información, (ii) permitir a las personas naturales el acceso a la información que se tenga sobre ellas en sus bases de datos, (iii) utilizar la información únicamente para los fines propuestos por la organización al momento de su recolección y (iv) cumplir con estándares de seguridad que garanticen que la información se encuentra debidamente protegida. A esta ley de protección de datos personales se deben acoger las empresas u organizaciones que realicen tratamiento de datos personales en Canadá[75].

> Hay una serie de requisitos para cumplir con la ley. Las organizaciones cubiertas por Pipeda generalmente deben obtener el consentimiento de una persona cuando recopilan, usan o divulgan la información personal de esa persona[76].

Adicionalmente: "Pipeda se aplica a organizaciones del sector privado en todo Canadá que recopilan, usan o divulgan información personal en el curso de una actividad comercial."[77]

El documento expedido por la Oficina del Comisionado de Canadá se trata del documento denominado *kit de herramientas de privacidad: una guía para empresas y organizaciones*-

[75] Office of the Privacy Commissioner of Canada. PIPEDA. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ Fecha de acceso: 9 de septiembre de 2019. Traducido por la autora.

[76] Office of the Privacy Commissioner of Canada. PIPEDA in brief. [Página Web] Disponible en Internet: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/. Fecha de acceso: 12 de agosto de 2019. Traducido por la autora.

[77] Ibídem.

Ley de protección de la información personal y documentos electrónicos de Canadá[78]. En él se determinan las medidas por las cuales las organizaciones pueden precisar que son responsables en relación con el tratamiento de datos personales. Dentro de los aspectos más destacables de esta guía se puede encontrar la responsabilidad como eje para las organizaciones.

Al respecto, se recomienda a las organizaciones desarrollar un programa de gestión de privacidad donde se tengan en cuenta los siguientes aspectos[79]:

a) Brindar a su oficial de privacidad designado apoyo por parte de la alta gerencia y la autoridad para poder intervenir en cuestiones de privacidad relacionadas con cualquiera de las operaciones de su organización.

b) Comunicar el nombre o título de esta persona interna y externamente (por ejemplo, en sitios web y publicaciones).

c) Analizar y documentar todas las prácticas de manejo de información personal, incluidas las actividades en curso y las nuevas iniciativas.

Como se aprecia, existen diversas herramientas que pueden servir de ayuda a las organizaciones al momento de estructurar los marcos regulatorios del principio de *accountability*. Varias legislaciones en el mundo han elaborado mecanismos que pueden ser de apoyo al momento de organizar el componente o programa integral de gestión de datos personales que proteja los datos de clientes y consumidores en una organización.

[78] Office of the Private Commissioner of Canadá Cat. No. IP54-58/2016ISBN 978-0-660-06541-0 Disponible en [PDF] 2015.

[79] Office of the Private Commissioner of Canadá. A guide for businesses and organizations. Privacy Toolkit. Canada´s Personal Information Act. Disponible en [PDF] Cat. No. IP54-58/2016 ISBN 978-0-660-06541-0. Diciembre del 2015. p 12. Fecha de acceso: 14 de agosto de 2019. Traducido por la autora.

Además, de acuerdo con el desarrollo de las nuevas tecnologías, surgen nuevas herramientas que sirven de base para lograr estructurar marcos legales de gestión de datos personales. Este es el caso de la analítica. Según Schwartz, este término: "(…) se refiere al uso de la tecnología de la información para aprovechar estadísticas, algoritmos y otras herramientas de matemáticas para mejorar la toma de decisiones"[80].

Al respecto, The Centre for Information Policy Leadership ha mencionado:

> Las analíticas prometen revolucionar los negocios, la ciencia, la investigación y la educación. Poderosos algoritmos ayudan a identificar a las personas o individuos que requieren servicios sociales, detectar fraudes, predecir los efectos de desastres naturales, reconocer patrones en la investigación científica y descubrir tendencias en la demanda del consumidor[81].

Adicionalmente, el valor agregado que representa consiste en que:

> Si bien la analítica tradicional se ha utilizado para encontrar respuestas a preguntas predeterminadas, su aplicación al *big data* (inteligencia de datos) permite la exploración de información para ver qué conocimiento puede derivarse de él, e identificar conexiones y relaciones que son inesperadas o que fueron previamente desconocidas[82].

---

[80] SCHWARTZ Paul, "Data Protection Law and the Ethical Use of Analytics. Citado por: Centre for Information Policy Leadership. Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance. A Discussion Document. February 2013. Traducido por la autora.

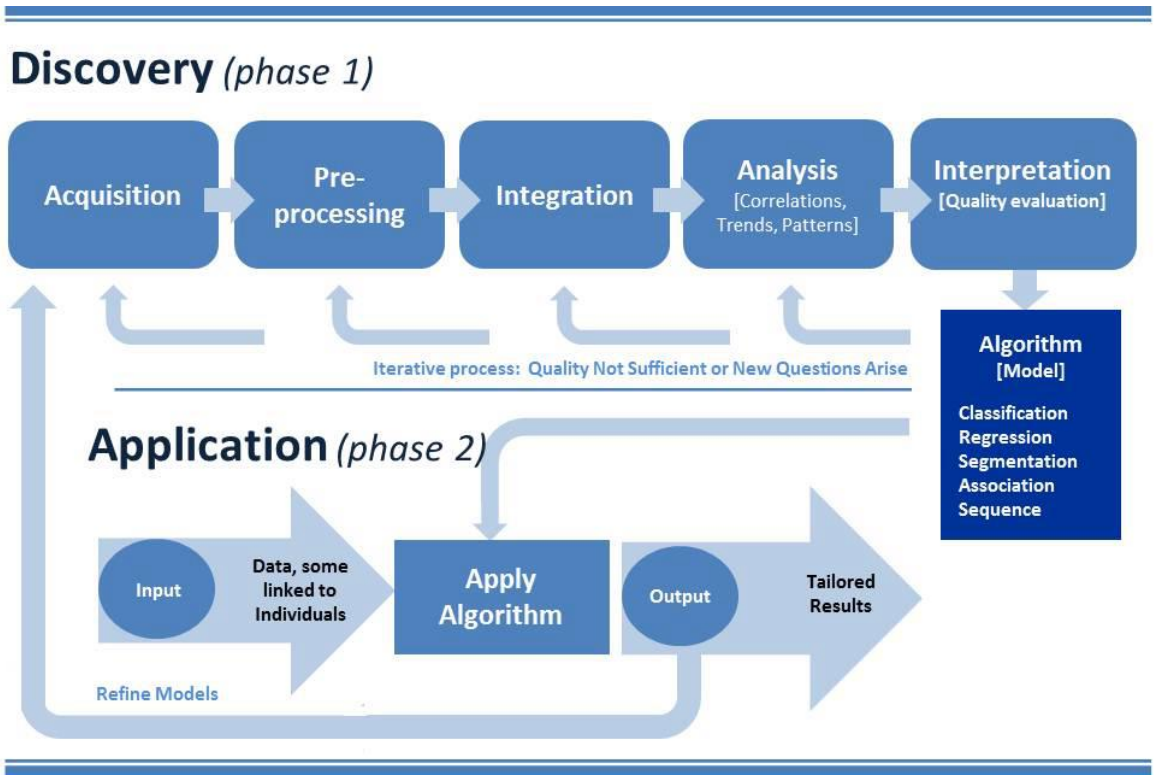
[81] Centre for Information Policy Leadership. Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance. A Discussion Document. [PDF] February 2013. P 1. Fecha de acceso: 11 de agosto de 2019.

[82] *Ibid*., P 1. Traducido por la autora.

El proceso que determina la implementación de la analítica en los negocios ha sido explicado por el Centre for Information Policy Leadership en dos fases, las cuales se analizan en inglés en la figura 1.

Figura 1

El proceso de la analítica



Fuente: Centre for Information Policy Leadership. Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance. A Discussion Document. P 8 [Consultado el 12 de agosto de 2019].

De acuerdo con lo anterior, las analíticas pueden considerarse como herramienta tecnológica para la gestión de *big data* y, en general, de procesos que conlleven recolección y tratamiento de datos personales, los cuales se desarrollan a través de dos fases principales. La primera, de descubrimiento, que conlleva:

> Descubrimiento de conocimiento que implica reunir datos para analizar, preprocesarlos en un formato que puede usarse, consolidándose para el análisis, analizándolo para descubrir qué puede revelar e interpretarlo para comprender los procesos mediante los cuales se analizaron los datos[83].

Adicionalmente, se observa una segunda fase de aplicación que implica el que:

> Una organización pueda, por ejemplo, clasificar a las personas según ciertos criterios, y al hacerlo determinar su idoneidad para participar en una actividad particular. Eso puede predecir lo que las personas pueden comprar o hacia dónde pueden viajar, y sobre esa base decidir qué comprarle[84].

Adicionalmente, para poder constituir marcos regulatorios que gestionen adecuadamente el principio de *accountability*, es posible contar con otros instrumentos como el *balance scorecard*. Se trata de una herramienta consistente en:

> Un cuadro de mando integral (BSC) es un método para analizar organizaciones y crear estrategias para cumplir los objetivos de la organización. Los cuadros de mando integrales alinean los objetivos y las estrategias de una organización con muchas medidas de desempeño y otros factores como la satisfacción del cliente, el desempeño financiero, la eficiencia interna y las innovaciones[85].

Para alcanzar un complemento entre el marco regulatorio y legal que gestione el principio de *accountability* en una organización y el desarrollo de este, para alcanzar los objetivos que reflejan que las medidas y estrategias tomadas por una organización pueden ser verificadas:

---

[83] *Idem,* p 9.

[84] *Idem,* p 10.

[85] DZIAK, Mark. Balanced scorecard (BSC). Salem Press Encyclopedia, 2018.

> (…) se ha vuelto más claro que para que la rendición de cuentas funcione debemos ser capaces de medir la efectividad de programas de privacidad y cómo se vinculan con los elementos esenciales. El principio de responsabilidad demostrada requiere que una organización sea responsable y, así mismo, responda[86].

Si bien es necesario estructurar una serie de medidas y estrategias internas que permitan gestionar el principio de *accountability* en las organizaciones, tales providencias se deben manifestar en marcos legales que incluyan este principio. No pueden ser solamente un conjunto de documentos que reflejen políticas de aplicabilidad de *accountability*, sino que es necesario y fundamental disponer de mecanismos de auditoría que permitan comprobar si efectivamente están produciendo los resultados esperados.

3.1.2 Marco regulatorio de Nymity

Existen diversos tipos de marcos regulatorios que pueden ayudar a las organizaciones a lograr estructurar sus políticas y directrices, encaminadas a una adecuada implementación del principio de *accountability*. Uno de ellos es el PMAF o Marco de Nymity[87].

> El Marco es integral, jurisdiccional e industrial y trabaja con programas de privacidad que son relativamente nuevos o muy maduros. Organizaciones alrededor del mundo están utilizando el marco para estructurar sus programas de privacidad. El PMAF es compuesto por trece procesos de gestión de

[86] MCQUAY Terry. The Privacy Office Guide to Demonstrating Accountability. p 1. Traducido por la autora.
[87] Compañía global líder en investigación especializada en cumplimiento normativo y en la implementación y gestión efectiva de programas de protección de datos personales. Nymity Innovating Compliance. Nosotros. © 2002-2017 Nymity Inc. All Rights Reserved. Disponible en Internet: https://latam.nymity.com/nosotros.asp. Fecha de acceso: 17 de agosto de 2019.

privacidad, cada uno de los cuales contiene múltiples actividades de gestión de privacidad (más de 150 en total)[88].

Dentro de los múltiples propósitos para lograr una adecuada implementación del principio de *accountability* con base en el PMAF se puede encontrar:

a) Estructuración del programa de privacidad: "Algunas organizaciones, a menudo aquellas con nuevo programa de privacidad o buscando mejorar su programa existente, han encontrado este marco efectivo para estructurar el programa de privacidad"[89]. El Marco es aplicable tanto a organizaciones nuevas que busquen estructurar su programa de privacidad, como para empresas que tengan un esquema regulatorio y quieran mejorarlo o complementarlo.

b) Planificación: "Algunas organizaciones utilizan el marco como lista de verificación para identificar las actividades de gestión de privacidad existentes y para planificar la implementación de las nuevas"[90]. El Marco presenta un listado de actividades de gestión de privacidad que permiten verificar aquellas que existen y las que requieren ser implementadas.

c) Evaluación comparativa: "Este Marco proporciona un mecanismo eficaz para comparar el programa de privacidad en diferentes áreas de la organización, o entre dos organizaciones"[91]. Los programas y marcos regulatorios de privacidad de la información deben aplicarse a las distintas áreas que existen en una organización. Es importante determinar cómo está prevista la aplicabilidad del Marco en otras organizaciones, teniendo en cuenta que a partir de aquí se pueden dar mejoras en relación con la eficiencia y eficacia del mismo.

[88] *Ibid*., P 60.

[89] *Idem,* P 60.

[90] *Idem,* P 61.

[91] *Idem,* P 61.

d) Informes reglamentarios: “Informar a un regulador es una forma de demostrar responsabilidad. Algunas organizaciones están utilizando este Marco para mostrar la debida diligencia, por ejemplo en el caso de una violación de datos para demostrar que el evento fue una excepción que ocurrió a pesar de un programa robusto para prevenirlo”[92]. Es importante que las organizaciones logren demostrar a los entes reguladores en materia de protección de datos personales. Esto se puede alcanzar a través de procesos de debida diligencia frente a los cuales el marco es una buena alternativa probatoria al respecto.

El PMAF fue desarrollado para comunicar el estado del programa de privacidad, en otras palabras para demostrar responsabilidad[93]. Este marco desarrolla los procesos determinados en la tabla 2.

Es preciso, entonces, que las empresas y organizaciones consideren las diversas variables relacionadas con el adecuado cuidado de datos personales, que pueden ayudar en la elaboración de marcos legales de protección de datos personales que permitan evidenciar la aplicabilidad del principio de *accountability*. Asimismo, las nuevas tecnologías brindan ayuda y soporte para la adecuada gestión de los marcos empresariales.

Los marcos conllevan, a su vez, una responsabilidad doble: por un lado, la prueba del cumplimiento de los estándares normativos establecidos por las múltiples legislaciones y, por el otro, comprobar que existe una correlación entre las medidas y estrategias que se encuentran plasmadas en los marcos legales y su real y efectiva eficacia en la práctica. Esto trae como consecuencia una debida gestión de datos personales de consumidores de comercio electrónico.

[92] *Idem,* P 61.

[93] MC QUAY Terry. The Privacy Office Guide to Demonstrating Accountability. [PDF] Copyright © 2014 by Nymity Inc. P 15.

Tabla 2

Procesos de gestión de privacidad

1. Mantener la estructura de gobierno
2. Mantener inventario de datos personales
3. Mantener la política de privacidad de datos
4. Insertar privacidad de datos en operaciones
5. Mantener programa de entrenamiento y conocimiento
6. Gestionar el riesgo de la seguridad de la información
7. Administrar riesgos de terceros
8. Mantener avisos
9. Mantener procedimientos para resolver quejas y reclamos
10. Monitoreo de nuevas operaciones prácticas
11. Mantener el programa de manejo del incumplimiento de la privacidad de datos
12. Monitorear las prácticas de manejo de datos
13. Seguimiento de criterios externos

Fuente: McQuay Terry. The Privacy Office Guide to Demonstrating Accountability. [PDF] Copyright © 2014 by Nymity Inc. p. 15.

3.2 Casos que evidencian vulneración de protección de datos personales en plataformas digitales

Ha quedado demostrado que la información personal se constituye, hoy por hoy, en activo para las empresas y organizaciones, dado el advenimiento de las nuevas tecnologías y el surgimiento de los negocios que requieren modelos operativos que funcionan con base en la gestión de datos personales de clientes y consumidores de comercio electrónico. En gigantes tecnológicos como Facebook, Instagram y Twitter, entre otras, y empresas como Amazon, Ebay o Google, al igual que plataformas digitales como Uber, Cabify, Airbnb y Rappi se ha hecho necesario realizar una auditoría y control.

3.2.1 Casos que evidencian uso indiscriminado de datos personales a escala mundial

El uso indiscriminado de los datos personales, por parte de algunas empresas y organizaciones, ha traído como consecuencia casos en los cuales han abusado de su uso. Como consecuencia, se han manifestado varios casos a nivel mundial en los que se ha visto comprometida la información personal de los usuarios. De acuerdo con el diario El Espectador, dentro de los casos más relevantes se encuentran[94]:

a) Yahoo en el año 2013, donde se vieron afectadas más de 3.000 cuentas de sus usuarios. Este caso puso en riesgo la compra de Yahoo por parte de Verizon.

b) Uber como gigante tecnológico y de emprendimiento digital tampoco escapó a la vulneración de sus sistemas. En el año 2017 reveló que, hacia finales del 2016, datos personales de 57 millones de usuarios fueron robados. Los datos incluían correo electrónico, nombre y número de teléfono. La empresa fue cuestionada por haber guardado esta información, ya que esto afectaba directamente a sus clientes.

[94] GREMMEL Robin, Los principales casos de robo de datos personales. [En línea] En: El Espectador. 15 de mayo de 2018. Fecha de acceso: 9 de septiembre de 2019.

c) La agencia de crédito Equifax también sufrió un ataque mediante el cual fueron robados datos sensibles de 147 millones de usuarios que la empresa tiene en Estados Unidos, Canadá e Inglaterra. Esta empresa tuvo varias demandas en relación con este caso, ya que se comprobó que sus sistemas de seguridad eran vulnerables. Además, se reveló de manera tardía el incidente.

d) Por su parte, la empresa estadounidense Target se vio envuelta en un caso de vulneración a sus sistemas de seguridad, donde se afectó a unos 10 millones de clientes y se filtraron datos como —nombre, dirección postal, número de teléfono y correo electrónico—.

Es así como la información de clientes y consumidores en algunas ocasiones se ha puesto en riesgo, lo cual constituye una violación directa al derecho fundamental de hábeas data. A continuación, se analizarán dos de esos asuntos, que evidencian la vulneración de este derecho y su correlativa sanción, teniendo en cuenta el impacto del mal uso de los datos personales en los consumidores.

3.2.2 Caso Facebook-Cambridge Analytica

Uno de los casos más reconocidos a nivel mundial acerca de filtración de datos personales en plataformas digitales es el asunto Facebook-Cambridge Analytica. Este demostró que en algunas ocasiones no existe control interno por parte de algunas organizaciones en relación con el adecuado manejo de la información personal.

El uso indiscriminado de la información personal puede acarrear consecuencias para las empresas u organizaciones que realizan recolección y tratamiento de datos personales. Estas se manifiestan en relación con el usuario o consumidor, la imposición de multas y sanciones por parte de los órganos competentes en materia de protección de datos personales, a escala mundial, y el impacto frente a las negociaciones o inversiones con otras empresas, lo cual puede generar efectos negativos para una organización.

> El 17 de marzo del 2018, diversos medios de comunicación revelaron que Cambridge Analytica, consultora de la campaña electoral del presidente Donald Trump, obtuvo y usó ilegalmente los datos personales de más de 50 millones de usuarios de Facebook, aunque días después se corrigió dicha información precisando que realmente se trató de un número de 87 millones de usuarios afectados. Se estableció que la red social permitió que las aplicaciones vinculadas a ella pudieran obtener datos personales no solo de los usuarios que las descargaban sino de todos sus amigos[95].

Conforme a lo descrito, el uso de una aplicación externa a Facebook que permitía la realización de un test, puso al descubierto que la red social Facebook no contaba con las medidas de seguridad adecuadas para la protección de datos de los usuarios. Adicionalmente, la información que se filtró a través de la aplicación fue utilizada con fines electorales para la campaña de Estados Unidos en el cual el candidato Donald Trump se estaba postulando a la presidencia.

> Ello a su vez va unido a una *molestia* generalizada dadas las controversias sobre su posible influencia en la elección del presidente Trump y en el Brexit, la divulgación de noticias falsas en la red social, los cuestionamientos a la ausencia de transparencia frente a los algoritmos que determinan qué contenido ven los usuarios, el reconocimiento de su poder más allá de los tradicionales medios de comunicación, su influencia política, etc.[96].

[95] MORALES NEIRA Mónica Lizet. Notas sobre el caso de Facebook y Cambridge-Analytica: modelos de negocio que se basan en la explotación de datos personales. [Página Web] Innovación y emprendimiento. Abril de 2018. Disponible en: https://propintel.uexternado.edu.co/notas-sobre-el-caso-de-facebook-y-cambridge-analytica-modelos-de-negocio-que-se-basan-en-la-explotacion-de-datos-personales/ Fecha de acceso: 18 de agosto de 2019.

[96] *Ibid.*

A partir de los hechos expuestos anteriormente es fundamental analizar este caso de vulneración al derecho de hábeas data de los usuarios de esta red social. Como primera medida, se observa que no se trata de un caso de filtración involuntaria de datos personales ajena a la red social.

> Por el contrario, se trata de prácticas reiteradas efectuadas por distintas empresas de tecnología (término genérico pero que incluiría, entre otras, a aquellas cuyo objeto es la minería de datos) cuyo modelo de negocio se basa en la explotación económica de datos, y en este caso particular de datos personales de los usuarios[97].

Si bien es cierto que existe una necesidad de recolectar datos para la efectiva operatividad de los nuevos modelos de negocios *on-line* o basados en plataformas digitales, entre los que se encuentra el comercio electrónico.

> (…) no se puede perder de vista que para el tratamiento (recolección, almacenamiento, uso, circulación y supresión) de datos personales existen regulaciones que buscan proteger los derechos de los titulares de tales datos, al ser considerados en muchos países (incluido Colombia) como derecho fundamental"[98].

Como consecuencia de lo anterior, se han iniciado investigaciones en varios países en contra de la red social Facebook, lo cual ha determinado varias sanciones que han sido impuestas a escala mundial, debido al manejo inadecuado de los datos personales de los usuarios, en este caso conocido como Facebook-Analytica. En el Reino Unido, por ejemplo, se sancionó con una multa de 500.000 libras (565.000 euros) por permitir una

[97] *Idem*.

[98] *Idem*.

violación de las leyes sobre protección de datos personales en relación con el escándalo de Cambridge Analítica"[99].

> La Oficina del Comisionado de Información (ICO, por sus siglas en inglés), el organismo que supervisa el cumplimiento de las reglas sobre protección de datos en el Reino Unido, señaló hoy que Facebook permitió que se violase la legislación al posibilitar el acceso a información de sus usuarios sin 'un claro consentimiento'[100].

En Colombia, de acuerdo con la Resolución 1321 del 2019 de la SIC:

> Dada la circulación transfronteriza que realiza Facebook de la información de los colombianos, las fallas de seguridad que suceden en otros países afectan o puede afectar la información de las personas residentes o domiciliadas en la República de Colombia, cuyos datos son recolectados y tratados por Facebook[101].

Y agregó:

> (…) la seguridad de la información es una condición crucial del tratamiento de datos personales. Una vez recolectados deben ser objeto de medidas de diversa

[99] Agencia EFE. El Reino Unido multa a Facebook por el escándalo de Cambridge-Analytica. [En línea] En: Agencia EFE. Octubre de 2018. Disponible en: https://www.efe.com/efe/america/portada/el-reino-unido-multa-a-facebook-por-escandalo-de-cambridge-analytica/20000064-3792293. Fecha de acceso: 28 de septiembre de 2019.

[100] *Ibid*., Agencia EFE. El Reino Unido multa a Facebook por el escándalo de Cambridge-Analytica.

[101] COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 1321 de 2019. Por la cual se imparten órdenes dentro de una actuación administrativa. Bogotá, D.C., 2019. P 5. Disponible en Internet en: http://www.sic.gov.co/sites/default/files/files/Noticias/2019/Res-1321-de-2019.pdf. Fecha de acceso: 19 de agosto de 2019.

índole para evitar situaciones indeseadas que pueden afectar los derechos de los titulares y de los mismos responsables y encargados del tratamiento de los datos[102].

De acuerdo con la decisión de la SIC, el criterio de seguridad tiene un carácter de tipo preventivo para la legislación colombiana. Siguiendo este criterio, existe una responsabilidad demostrada que se manifiesta a través del principio de *accountability* y que le exige a las organizaciones reforzar las medidas de seguridad internas que permitan garantizar seguridad en el manejo de los datos personales.

Precisa la entidad que las medidas de seguridad no solo deben ser tomadas al momento de evidenciarse la ocurrencia de un fallo o filtración de datos personales. De acuerdo con la regulación y normativa colombiana, esta seguridad debe probarse de acuerdo con las normas colombianas, en este caso debe presentar concordancia con la Ley 1581 del 2012.

De esta forma, la SIC determinó que para lograr implementar el principio de *accountability* es necesario: "Implementar acciones de diversa naturaleza para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales". Además, las medidas de autorregulación para lograr implementar adecuadamente el principio de *accountability*: "Pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológicas, humanas y de gestión, que involucran procesos y procedimientos"[103].

La SIC analizó las investigaciones y los pronunciamientos de autoridades mundiales en materia de protección de datos personales, donde se evidencian fallas con relación a la recolección, el manejo y el tratamiento de los datos personales de los usuarios de la red social Facebook. Como consecuencia y teniendo en cuenta que existe un impacto en los usuarios colombianos en materia de datos personales, la entidad determinó que Facebook

[102] *Ibid*., p 22.

[103] *Idem,* p 24.

debe acoger las disposiciones establecidas por el principio de seguridad en Colombia y de esta forma asegurar la seguridad de los datos personales evitando conductas fraudulentas[104].

Agregó, además, que para lograr cumplir con lo establecido bajo el principio de seguridad en Colombia era preciso que Facebook fortaleciera las estrategias de seguridad a la fecha de expedición de su resolución. Por otro lado, la SIC estableció[105] que Facebook debía desarrollar un programa integral de gestión que permitiera evidenciar la confianza y la entereza de los datos personales, evitando la falsificación o uso inadecuado. Esta planificación debía constar por escrito y estar sujeta a verificaciones para comprobar su eficacia.

3.2.3 Caso Rappi

Conforme al desarrollo de nuevos esquemas y modelos de negocio *on-line*, en Colombia han surgido varias empresas que realizan negocios a través de plataformas digitales. Una de estas compañías es Rappi, la cual se vio involucrada en un caso de vulneración de datos personales.

> El operador a través de la plataforma realiza las siguientes acciones: i) exhibe diferentes productos y servicios de consumo de forma publicitaria para que puedan servir de referencia a los consumidores, ii) facilita el encuentro entre consumidores y mandatario para la realización del vínculo contractual, iii) permite el uso de la plataforma de pagos iv) sirve de medio de envío de comunicaciones entre los consumidores y los mandatarios[106].

---

[104] *Idem*, p 26.

[105] *Idem*, p 27.

[106] RAPPI. Términos y condiciones de uso de la Plataforma Rappi. [En línea] Legal.Rappi. Disponible en: https://legal.rappi.com/colombia/terminos-y-condiciones-de-uso-de-plataforma-rappi-2/?_ga=2.212683730.718552052.1566567140-410606911.1566567140. Fecha de acceso: 23 de agosto de 2019.

Como se observa, el núcleo central de los negocios que realiza Rappi es la venta de productos y servicios a través de la plataforma de comercio electrónico, siendo un proveedor directo a los consumidores. Aquí se evidencia la génesis del comercio electrónico, frente a la cual se elimina el fenómeno de intermediación y se realizan los negocios de manera directa, haciendo uso de las plataformas digitales y las aplicaciones.

En relación con el uso de los datos personales, se presentó una queja ante la SIC, entidad que inició una investigación para verificar si existió vulneración al derecho fundamental de hábeas data[107]. La entidad inició investigación conforme a los siguientes hechos: el día 3 de noviembre del 2016, un consumidor de la plataforma presentó queja ante Rappi para solicitar la supresión de sus datos personales en relación con el envío de mensajes de texto a su celular y correo electrónico.

Dentro de las investigaciones realizadas por la delegatura de protección de datos de la SIC se encontró que Rappi no contaba con la autorización del titular de datos personales. Teniendo en cuenta que a pesar de que la empresa indicó que sus consumidores deben aceptar los términos y condiciones para poder hacer uso de la plataforma, en ningún momento allegó prueba o soporte de dicha aceptación por parte de titular de los datos. Asimismo, la delegatura consideró que la compañía probablemente no garantizó el derecho de hábeas data, teniendo en cuenta que siguió realizando tratamiento de los datos del consumidor, a pesar de la solicitud de supresión por parte del consumidor de comercio electrónico.

El organismo de vigilancia y control estableció que en este caso se transgredieron las regulaciones y los intereses establecidos por la Ley 1581 del 2012, teniendo en cuenta que efectivamente fue probada la vulneración del derecho de hábeas data por parte de Rappi SAS[108]. En efecto, no se suprimieron efectivamente los datos del consumidor conforme a lo

[107] COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 9800 de 2019. p 1.

[108] *Ibid.*, p 13.

establecido por la regulación colombiana, ni tampoco se logró demostrar que contaba con la autorización del titular para poder recolectar y realizar tratamiento de sus datos personales.

De acuerdo con el análisis que realizó la SIC en el presente caso, determinó una sanción para Rappi por un valor de 298.121.760 pesos. Además, procurando la implementación adecuada del principio de *accountability*, la SIC le ordenó a la empresa: (i) abstenerse de comunicarse con titulares de datos personales con los cuales no tenga autorización previa y expresa, (ii) identificar plenamente a sus usuarios mediante la plataforma de comercio electrónico o a través de la aplicación, (iii) en el momento en el cual un titular de datos personales solicite que sus datos sean suprimidos, la empresa debe cumplir con ello, (iv) conservar prueba de la autorización emitida por los titulares de datos personales y (v) poner a disposición de los titulares de datos personales mecanismos ágiles que permitan suprimir sus datos o la revocatoria del consentimiento de tratamiento de datos personales.

Después de analizar estos casos, es evidente que las empresas y organizaciones se encuentran en el deber de cumplir con lo establecido por la normativa relacionada con protección de datos personales. Las buenas prácticas en esta materia se pueden constatar por el uso y gestión de herramientas que permitan medir si efectivamente las estrategias, políticas y documentos dentro son correlativos con la práctica. El principio de *accountability* exige una conexidad entre las medidas internas y la puesta en práctica de estas, para demostrar efectividad.

Como parte de diligenciar medidas de derecho preventivo, es preciso que las organizaciones logren establecer marcos legales y programas integrales que puedan gestionar adecuadamente el derecho de hábeas data. De esta forma, se pueden evitar fuertes sanciones económicas por parte de los organismos que tienen a su cargo su regulación y procesos que conllevan tiempo y dinero y que pueden afectar a las empresas.

Las nuevas tecnologías facilitan el desarrollo de los negocios que permiten un impacto en nuevos mercados y nuevos consumidores. Sin embargo, conllevan una responsabilidad frente a los datos y la información personal de los consumidores de comercio electrónico.

3.3 Medidas para lograr la efectiva protección del consumidor de comercio electrónico bajo el principio de 'accountability'

Los nuevos modelos de negocio que desarrollan empresas y organizaciones que hacen negocios internacionales, requieren información personal por parte de los consumidores. En este contexto, existe una responsabilidad por parte de las organizaciones en relación con la recolección, y tratamiento de los datos personales. Como consecuencia, es vital crear medidas de tipo preventivo que busquen mitigar y minimizar al máximo los riesgos que se derivan de un tratamiento inadecuado de datos personales.

> Con la aparición de Internet y el desarrollo de nuevos servicios de comunicación e información en línea se han ido incrementando las posibilidades de recogida y tratamiento de ingentes cantidades de información sobre las personas. La información se ha transformado en un bien básico para las sociedades y para el funcionamiento de la economía[109].

3.3.1 Principio de 'accountability' de acuerdo con lo dispuesto por la OCDE

Para determinar las mejores estrategias encaminadas a la debida diligencia y elaborar programas integrales que abarquen marcos legales regulatorios y probatorios del principio de *accountability* es posible utilizar herramientas tecnológicas ofrecidas por las TIC. Si bien es cierto que este fue desarrollado por la OCDE,

[109] DOMÍNGUEZ GARRIGA, Ana. MOTORES DE BÚSQUEDA, REDES SOCIALES, RASTRO DIGITAL Y PUBLICIDAD COMPORTAMENTAL. En: NUEVOS RETOS PARA LA PROTECCIÓN DE DATOS PERSONALES En la Era del *big data* y de la computación ubicua. Editorial DYKINSON, S.L. Meléndez Valdés, 61-28015 Madrid. 2015. PP 36 y 37.

> (…) la relevancia que están tomando los datos de los consumidores explica que se les esté asociando con 'el petróleo del siglo XXI', en el sentido de que podrían ser la materia prima más valiosa y necesaria para una compañía moderna[110].

De acuerdo con lo anterior, y realizando un análisis acerca del principio de *accountability*, es evidente que este postulado tiene una exigencia doble en relación con su debida aplicación: por una parte, es preciso que las organizaciones puedan lograr esquematizar programas integrales de protección de datos personales que incluyan marcos de gestión y protección adecuada de la información de consumidores de comercio electrónico. Por la otra, es necesario que los programas incluyan herramientas tecnológicas que permitan medir la adecuada gestión de los marcos y su real eficacia y eficiencia en la práctica. De esta forma, es posible generar confianza en el consumidor respecto del manejo y tratamiento de sus datos personales y lograr una fidelización por parte de los clientes frente a esa seguridad que ofrece el manejo adecuado de sus datos personales.

Conforme a los nuevos modelos de negocio digital

> (…) hay mucha obsesión por recoger *data*, pero la obsesión debería estar en qué hago con estos datos para que me ayuden a fidelizar al cliente, ofrecerle mejores productos y lograr una repercusión positiva en mi negocio[111].

Considerar la protección óptima de datos personales de consumidores de comercio electrónico también puede conducir a un mejor posicionamiento de las empresas y organizaciones.

---

[110] Finanzas.com Google: Aunque los datos son el nuevo petróleo, la clave es saber activarlos**.** [En línea] Finanzas.com 25/06/2019. Disponible en: http://www.finanzas.com/noticias/empresas/20190625/google-aunque-datos-nuevo-4020859.html. Fecha de acceso: 25 de agosto de 2019.

[111] *Ibid.*

De acuerdo con los avances que presenta la tecnología en nuestros días, existen algunas legislaciones que han comenzado a regular una protección de datos personales 2.0, lo que equivale a determinar mecanismos mediante los cuales las empresas que operen en un ecosistema digital puedan implementar y cumplir a cabalidad con lo establecido por el principio de *accountability*. Más adelante, se analizará una propuesta para regular este tema en un ecosistema digital.

3.3.2 Avances sobre proyectos legislativos regulatorios frente al principio de 'accountability' en Estados Unidos

El documento *Deceptive Experiences to on-line Users Reduction (Detour) Act* representa un gran hito en la protección de la privacidad de los usuarios en internet y al incremento de la supervisión de las prácticas de las grandes compañías tecnológicas. Junto con el proyecto de la responsabilidad algorítmica —*Algorithmic Accountability Act*—, que se tratará a renglón seguido, forman parte del grupo de medidas que revolucionan el uso de la tecnología[112].

El objetivo del proyecto de *Detour Act* "es prohibir que las grandes empresas tecnológicas utilicen determinadas interfaces y diseños engañosos conocidos como *dark patterns*"[113]. En Internet, su uso puede vulnerar una política de privacidad y generar efectos con respecto al conocimiento de lo que se adquiere a través de las plataformas de comercio electrónico, así como viciar el consentimiento de los usuarios[114].

---

[112] SMART LAW. DETOUR Act: la revolución del uso de la tecnología en los próximos años [En línea] En: The Technolawgist. junio 4, 2019. Disponible en: http://www.thetechnolawgist.com/2019/06/04/detour-act-revolucion-us-de-la-tecnologia-en-los-proximos-anos/. Fecha de acceso: 25 de agosto de 2019.

[113] *Ibid.* SMART LAW. DETOUR Act: la revolución del uso de la tecnología en los próximos años.

[114] "En palabras del senador Fischer, "cualquier política de privacidad que implique la prestación de consentimiento se ve debilitada por la presencia de *dark patterns*". "Estas interfaces de usuario manipuladoras limitan intencionalmente la comprensión y socavan la capacidad de elección del consumidor. De acuerdo con lo mencionado en el artículo: SMART LAW. DETOUR Act: la revolución del uso de la tecnología en los próximos años.

De acuerdo con lo anterior, cuando los consumidores se encuentran debidamente informados pueden tomar mejores decisiones en relación con el producto o servicio que están adquiriendo. De esta forma, se busca evitar que se utilicen interfaces como los *dark patterns*, los cuales son considerados "trucos utilizados en sitios web y aplicaciones que pretenden que un usuario haga cosas que no quiere como comprar o registrarse para algo"[115]. En tal medida, pueden limitar la capacidad de elección del consumidor de comercio electrónico.

Según se anticipó, el *Algorithmic Accountability Act —Ley sobre Responsabilidad Algorítmica—* tiene por objetivo: "obligar a las grandes empresas a analizar de forma periódica sus algoritmos y reparar aquellos algoritmos que generen decisiones discriminatorias, injustas, sesgadas o imprecisas"[116]. Este proyecto de ley es aplicable al ámbito federal y, por lo tanto, aplicable territorialmente a Estados Unidos.

Dentro de los aspectos más destacables frente a la debida protección de datos personales se observa que este proyecto de ley:

> Exige a las empresas que evalúen el uso y el impacto de sistemas de decisiones automatizadas, incluyendo los datos utilizados para el entrenamiento de algoritmos, con el fin de determinar la precisión, imparcialidad de estos sistemas; identificar posibles sesgos, resultados discriminatorios y medir la protección de la privacidad y las medidas de seguridad (…). Exige a las empresas que evalúen cómo sus sistemas de información protegen la privacidad y la seguridad de los datos personales de los consumidores[117].

---

[115] DARK PATTERNS. Disponible en: https://www.darkpatterns.org/

[116] SMART LAW. Algorithmic Accountability Act: así se está regulando el futuro del *big data* y los algoritmos en Estados Unidos. [En línea] En: The Technolawgist. junio 3, 2019. Disponible en: http://www.thetechnolawgist.com/2019/06/03/algorithmic-accountability-act-regulando-el-futuro-big-data-los-algoritmos-estados-unidos/ Fecha de acceso: 25 de agosto de 2019.

[117] *Ibid.*

En búsqueda de la consolidación de prácticas que reflejen una adecuada implementación del principio de *accountability* para modelos de negocios digitales, empresas como Google se encuentran desarrollando sistemas que puedan lograr esta meta. Al respecto, propone:

> Para evitar huellas dactilares que permiten identificar que su máquina sea identificable como suya, Google propone la idea de un presupuesto de privacidad. Con esto, un navegador podría permitir que los sitios web realicen suficientes llamadas a la API para obtener suficiente información suya para poder agruparla en una cohorte mayor, pero no hasta el punto en el que abandone su anonimato. Una vez que un sitio ha agotado este presupuesto, el navegador deja de responder a cualquier otra llamada[118].

Este sistema está orientado a un bloqueo de las *cookies* a través de la web, lo cual crea dificultades para los expertos en *marketing* y publicistas al momento de intentar rastreos de consumidores de comercio electrónico, al momento de realizar sus consultas en Internet. Como consecuencia, se personaliza el uso de las *cookies* para lograr que cada usuario tenga mayor seguridad y privacidad.

Conforme a lo expuesto, esta tecnología permite realizar perfiles de consumidores frente a preferencias de adquisición de productos o servicios, por lo cual, legislación norteamericana busca equilibrar la capacidad para que los consumidores de comercio electrónico puedan tomar las mejores decisiones al momento de adquirir un producto o servicio. Esto constituye un avance significativo con miras a regular el manejo y la gestión de los datos personales y, además, exige a las organizaciones tener mayores y mejores estándares en el manejo de sistemas de información que consoliden el motor de este tipo de negocios en la web.

---

[118] LARDINOIS Frederic. Google Proposes new privacy and anti-fingerprinting controls for the web. [En línea] En: Techcrunch. 22 de agosto de 2019. Disponibilidad: https://techcrunch.com/2019/08/22/google-proposes-new-privacy-and-anti-fingerprinting-controls-for-the-web/. Fecha de acceso: 25 de agosto de 2019.Traducido por la autora.

3.3.3 Herramientas tecnológicas que permiten una adecuada implementación del principio de 'accountability'

Las organizaciones y empresas que realizan negocios digitales tienen grandes desafíos frente a la oportuna protección de los datos personales de los consumidores de comercio electrónico. Una de las mayores problemáticas se evidencia con la génesis de los modelos de negocio *on-line*, que requieren información personal para su funcionamiento. Por esto, es fundamental determinar medidas y estrategias que permitan gestionar de la mejor forma la información y darle la protección conveniente.

De acuerdo con Willemsen:

> Los requisitos de privacidad tienen un impacto en la implementación de nueva tecnología, y muchas implementaciones fallarán con el tiempo ya que no abordan de manera insuficiente los principios de privacidad por diseño y protección por defecto[119].

Conscientes de estos requerimientos y de los cambios y transformaciones que devienen en los negocios, como consecuencia de las actividades comerciales que se realizan a través de plataformas, existen organizaciones que están comenzando a visibilizar transformaciones en relación con la gestión de datos personales. De acuerdo con el vicepresidente de la compañía Virtru[120], Robert Macdonald[121], al mirar el panorama que concierne al cumplimiento de los programas de privacidad, la empresa desarrolló:

---

[119] VIRTRU. Why Virtu. Gartner, Predicts 2019: The Ambiguous Future of Privacy, Bart Willemsen, Daryl Plummer, et al., 14 November 2018. Disponible en: https://www.virtru.com/about/ Fecha de acceso: 25 de agosto de 2019. Traducido por la autora.

[120] Se trata de una empresa de cifrado de correo y privacidad digital. Disponible en: https://www.virtru.com/. Fecha de acceso: 28 de septiembre de 2019.

[121] CHIAVETTA Ryan. Solution helps developers embed privacy into applications. [En línea] En: IAPP. 15 de agosto de 2019. Disponible en: https://iapp.org/news/a/solution-helps-developers-embed-privacy-into-applications/ Fecha de acceso: 25 de agosto de 2019. Traducido por la autora.

> (…) una solución diseñada para proteger la información personal en posesión del propietario de los datos, permitiéndoles implementar líneas de código en sus aplicaciones personalizadas para garantizar que todos los datos regulados que tienen sean seguros[122].

Teniendo en cuenta el potencial que pueden ofrecer algunas herramientas para la adecuada gestión y protección de datos personales, es preciso tomar como ejemplo lo realizado por Virtru y mencionar algunas de ellas, las cuales contribuyen en la efectiva búsqueda de correcta aplicación del principio de *accountability* para lograr una correcta protección de los datos de consumidores de comercio electrónico.

3.3.4 Arquitectura de encriptamiento de datos personales

Uno de los mecanismos que permite gestionar y tratar adecuadamente la información se trata del centro de desarrolladores de la empresa Virtru, mencionada anteriormente. Ese centro les permite a los titulares de la información determinar quién tiene acceso a su información y hasta cuándo puede hacerlo, además de disponer a qué información pueden tener acceso los terceros. De acuerdo con Mac Donald[123], Virtru ha realizado esfuerzos para servir de guía a empresas y organizaciones para lograr el cumplimiento —*compliance*— que exigen los requerimientos universales.

El esquema o la arquitectura bajo la cual opera uno de los productos de Virtru, conocido como "Virtru Developer Hub", permite que el equipo de ingeniería logre implementar protección de datos personales a las aplicaciones que desarrollen las empresas.

> Al abrir nuestra plataforma de protección de datos de confianza cero, comprobada para proteger a más de 5.000 clientes, Virtru elimina la carga de

[122] *Ibid*, CHIAVETTA Ryan. Solution helps developers embed privacy into applications.

[123] *Idem*.

> crear soluciones de cifrado para que los desarrolladores puedan centrarse en crear aplicaciones para satisfacer las necesidades comerciales[124].

Este producto tecnológico va más allá de un encriptamiento de datos para garantizar la protección de la información. Ahora, es posible que el equipo de desarrolladores de aplicaciones que son importantes para la organización, puedan aplicar una debida protección de datos personales a las aplicaciones directamente, lo cual puede llegar a considerar una debida protección tanto de la información que tiene la empresa, como de aquella que pertenece al plano personal de los clientes y consumidores de comercio electrónico.

3.3.5 'Balance score card'

Se trata de un marco pragmático, escalable y basado en evidencia que les permite a las organizaciones demostrar responsabilidad mediante el monitoreo, la medición y la presentación de informes sobre las actividades continuas de gestión de la privacidad. El cuadro de mando se basa en los tres elementos clave de la responsabilidad descritos en capítulos anteriores: responsabilidad, propiedad y evidencia[125].

La empresa Nymity ha desarrollado la manera como opera este *balance scorecard*, cuya estructura se muestra en inglés en la figura 2.

[124] VIRTRU. Virtru Developer Hub. Disponible en: https://www.virtru.com/data-encryption-sdk/. Fecha de acceso: 25 de agosto de 2019. Traducido por la autora.

[125] MCQUAY Terry. The Privacy Office Guide to Demonstrating Accountability. Op. cit, p 28. Traducido por la autora.

Figura 2

Proceso 'balance scorecard'

Fuente: McQuay Terry. The Privacy Office Guide to Demonstrating Accountability. [Consultado el 25 de agosto de 2019]

Para comprender el funcionamiento del *scorecard*, a continuación, se estudiarán sus aspectos más importantes:

a) Identificación y categorización de las acciones de gestión de privacidad. Es necesario que el área que maneja los temas de privacidad dentro de la organización identifique las acciones de gestión de privacidad. Estas labores pueden hacer parte del núcleo esencial de privacidad o pueden ser de tipo electivo.

b) Determinar propiedad y frecuencia: para cada actividad de privacidad, se debe determinar un propietario y una frecuencia. Al hablar de propietario se hace referencia a la oficina de privacidad. La frecuencia se refiere principalmente a las actividades de privacidad, su desarrollo de manera periódica o continua.

c) Preguntas de recolección de evidencia: para cada actividad de gestión de privacidad, es necesario realizar unas preguntas que recojan la evidencia de los propietarios de la información.

d) Recolectar evidencia: una vez el cuadro de mando o *scorecard* se encuentre establecido por la oficina de privacidad, el siguiente paso es recolectar evidencia. Esto se puede realizar a través de preguntas que se establecen en el programa integral de gestión de datos personales.

e) Cálculo de puntaje de responsabilidad de privacidad de datos: el puntaje de responsabilidad de privacidad de datos representa el estado del programa de privacidad como un porcentaje de las actividades básicas y electivas de gestión de privacidad que se han completado y evidenciado de manera continua[126]. La puntuación se calcula mediante la división del número de actividades para las cuales el titular ha proporcionado evidencia —es decir, "La respuesta es sí—, por la cantidad de actividades identificadas por la oficina de privacidad. El resultado es igual al porcentaje de actividades que se evidencian a partir de esa fecha específica[127]. Se trata de una fórmula mediante la cual se divide el número de actividades de gestión de privacidad, donde el titular de datos ha respondido sí, en la cantidad de actividades que han sido identificadas por la oficina de privacidad.

f) Administración del *scorecard*: las actividades de gestión de privacidad deben ser continuas, adicionalmente, la evidencia debe estar actualizada. Este cuadro de mando o *scorecard* es orgánico y debe actualizarse de manera periódica, bien sea de forma mensual, semestral o anual.

3.3.6 SGSDP

Permite la interacción entre un grupo de actividades y elementos que buscan establecer y lograr metas en relación con la gestión adecuada de protección de datos personales. Así, se define como un:

> Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y

[126] *Idem*, p 31.

[127] *Idem*, p 31.

responsabilidad previstos en la ley, su reglamento, normativa secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia[128].

La estructuración del sistema de gestión permitirá que las organizaciones cumplan con estándares internacionales en materia de datos personales. Algunos de ellos se listan en el cuadro 1.

3.4 Estrategias jurídicas y herramientas tecnológicas para una adecuada implementación del principio de 'accountability'

Para lograr la eficacia real de las políticas y medidas que determine una organización, es necesario estructurar un sistema híbrido que combine medidas regulatorias para la adecuada gestión y protección de datos personales. Igualmente, se hace preciso crear herramientas tecnológicas que sirvan de instrumentos de colaboración para lograr eficacia y eficiencia de las medidas y políticas que determine la organización al momento de estructurar e implementar el principio de *accountability* en la praxis.

De la misma manera en la cual se ha venido consolidando una RSE, consecuencia del surgimiento de nuevos modelos de negocios, tanto analógicos como digitales, también surge el concepto "responsabilidad digital corporativa", para lograr un adecuado manejo de los datos en un ecosistema digital y los dispositivos que han sido creados a través de la tecnología. En este punto es importante que las empresas y organizaciones logren determinar el potencial que representan los datos personales para sus modelos de negocio. A partir de aquí, se pueden estructurar medidas de negocio que creen una sinergia entre el desarrollo de los modelos de negocios de empresas que realizan negocios a través de comercio electrónico y el adecuado tratamiento de los datos del consumidor.

[128] IFAI Transparencia y Privacidad. Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales. Marzo 2014. P 4.

Cuadro 1

Estructuración del sistema de gestión en relación con estándares internacionales

- BS 10012:2009 Data protection – Specification for a personal information management system
- ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.
- ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls.
- ISO/IEC 27005:2008, Information Technology–Security techniques– Information security risk management.
- ISO/IEC 29100:2011 Information technology – Security techniques – Privacy Framework
- ISO 31000:2009, Risk management – Principles and guidelines
- ISO GUIDE 72, Guidelines for the justification and development of management systems standards
- ISO GUIDE 73, Risk management – Vocabulary
- ISO 9000:2005, Quality management systems -- Fundamentals and vocabulary
- NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
- OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.

Fuente: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) Guía para implementar un sistema de gestión de seguridad de datos personales [PDF] Marzo 2014. [Consultado el 26 de agosto de 2019]

Es así como se hace necesario que las empresas y organizaciones tengan conocimiento acerca del derecho fundamental de hábeas data y, correlativamente, los deberes que tienen a su cargo por el hecho de recolectar y realizar tratamiento de datos personales. A partir de la importancia que reviste este derecho en relación con los consumidores, se deben crear programas integrales de gestión de datos personales que permitan demostrar, en la práctica, el uso adecuado que la organización otorga a los datos que pertenecen a los consumidores del comercio electrónico.

Es fundamental que los programas integrales de gestión determinen las bases para lograr buenas prácticas corporativas en materia de protección de datos personales. De acuerdo con las guías que han sido elaboradas por diversos organismos que regulan la protección de datos a escala mundial, es importante tener en cuenta las siguientes recomendaciones para crear un adecuado programa de gestión integral de protección de datos personales:

En primer lugar, es posible plantear estrategias jurídicas de *compliance* que permitan medir su eficacia y con la utilización de herramientas tecnológicas, que refuercen los esquemas y estructuras de recolección y tratamiento de datos personales de los consumidores de comercio electrónico y que garanticen su buen uso.

Conforme a lo anterior, es necesario crear un programa de gestión integral de privacidad. Este esquema puede gestionarse dese el área de gerencia y con ayuda del área administrativa. Una vez se determinen sus lineamientos es fundamental crear un departamento destinado a la protección de datos personales que se encargue de la gestión y regulación de la recolección y tratamiento de datos. A su vez, es importante designar el cargo de oficial de privacidad, funcionario que se encargará de intervenir en los asuntos de privacidad de la organización.

En segundo término, es fundamental analizar y documentar la información personal que tiene a su cargo la organización. Esta labor se puede realizar de forma física o digital a través de la gestión de bases de datos. Lo recomendable es gestionarlas a través de sistemas de información que permitan tener un mejor control. Para ello, es posible acudir a listas de chequeo que permitan determinar cuáles son aquellas actividades que la organización tiene en relación con la privacidad de los datos personales y qué requiere para lograr una adecuada protección de los datos. Esta lista puede ser variable, ya que a medida en que se consolidan nuevas bases de datos y actividades puede haber cambios.

Para cumplir a cabalidad con lo dispuesto por el principio de *accountability*, es indispensable solicitar autorización a los clientes para la recolección y el tratamiento de sus

datos. Esta prueba del consentimiento debe ser debidamente conservada por la empresa, al momento de ser requerida por alguna autoridad encargada de vigilar y proteger datos personales. En el caso de las organizaciones que desarrollan negocios a través de comercio electrónico es importante desarrollar un documento que gestione los términos y condiciones de uso de la plataforma digital o de la aplicación, que permita a los consumidores conocer los productos y servicios que ofrece la empresa y las condiciones mediante las cuales podrán acceder a dicha función.

Como tercera medida, es importante crear una política de privacidad que regule el tratamiento de los datos personales conforme a las regulaciones exigidas por el país en el cual la empresa se encuentre desarrollando sus negocios. Las diversas legislaciones tienen normativas y estándares distintos que se deben cumplir. Además, es importante implementar las medidas necesarias para ejecutar los estándares en materia de transferencias internacionales de datos personales.

Finalmente, en relación con las políticas jurídicas para la implementación y adecuación del principio de *accountability* es importante determinar un sistema de análisis y detección temprana de riesgos, frente a la información personal de los consumidores. Con ello se evita el incumplimiento de las regulaciones que permiten salvaguardar la información únicamente para los fines de la organización.

Además de la aplicación de herramientas tecnológicas y jurídicas, es importante considerar la administración del programa integral de gestión de datos personales, a través de marcos regulatorios estructurados a partir de arquitectura de cifrado de datos. Este permite que la información personal quede almacenada directamente en el dispositivo y, de esta forma, el consumidor de comercio electrónico puede tener un mayor control de su información. Para la implementación y uso adecuado de este tipo de tecnología es clave que los desarrolladores de una organización conozcan este tipo de cifrado y puedan aplicarlo a sus aplicaciones y servicios.

Por otro lado, es posible estructurar programas integrales de gestión de datos personales a partir del cuadro de mando o *balance scorecard* que permite la gestión de datos personales a través de mediciones que determinan si el programa efectivamente está evidenciando las medidas y estrategias de la organización en la práctica. Asimismo, es posible hacer uso de *blockchain*.

> Es una gran base de datos descentralizada en la que se ingresan diferentes tipos de datos como transacciones, procesos, acuerdos, datos personales, entre otros, los cuales pueden estar cifrados bajo operaciones matemáticas complejas, para aumentar la seguridad[129].

Son dos elementos los que caracterizan a este tipo de base descentralizada: el sistema de encriptación de datos que permite la confiabilidad en su tratamiento y la posibilidad de que sea pública o privada.

> *Blockchain* proporciona infraestructura donde la confianza en las transacciones no es negociada por intermediarios —como ha sido el caso hasta ahora— pero es incorporada de forma algorítmica en la operación. El proceso de consenso algorítmico es el agente de confianza. Su efectividad puede ser mejorada aún más, si se combina con el uso de *smart contracts* y *digital compliance*[130].

3.5 Conclusiones del capítulo

Las empresas y organizaciones que realizan diversas actividades a través de plataformas tecnológicas deben considerar la importancia y relevancia de una adecuada protección y

[129] Universidad Sergio Arboleda. En la Sergio. ¿Qué es Blockchain y por qué es el futuro de la seguridad de datos? Disponible en: https://www.usergioarboleda.edu.co/noticias/blockchain-la-seguridad-datos/. Fecha de acceso: 28 de septiembre de 2019.

[130] INTERNATIONAL FINANCE CORPORATION. WORLD BANK GROUP. Blockchain: Opportunities for Private Enterprises in Emerging Markets. January 2019. P 14.

cuidado de los datos de los consumidores de comercio electrónico. Un apropiado tratamiento de la información personal genera confianza y seguridad frente a la percepción que estos pueden tener, lo cual se puede traducir en fidelización de clientes.

El principio de *accountability* impone deberes para las organizaciones. El más importante de ellos es la responsabilidad frente las medidas y estrategias que puede tomar la organización para estructurar su programa integral de protección de datos personales y la demostración acerca de la eficacia y eficiencia de las medidas en la práctica. No se trata de un postulado que busque crear marcos regulatorios de papel. Las empresas deben probar que las medidas concuerdan con los resultados en la práctica y que esas políticas logran proteger adecuadamente a los consumidores.

Comprender los avances tecnológicos permite conocer qué herramientas existen y cómo pueden ayudar a estructurar los programas integrales de protección de datos personales. Su importancia radica en los nuevos negocios digitales que imponen cargas frente a la gestión y tratamiento de la información de los consumidores. No se trata de percibir al consumidor como una persona que solo demanda bienes o servicios y que hace parte de la etapa final del proceso productivo de una organización. Se busca comprender la importancia de su derecho a la privacidad y a la protección de datos personales.

Las organizaciones pueden considerar esquemas híbridos para el desarrollo de sus programas integrales de gestión de datos personales. Esto, permite regular dos ejes importantes de la implementación del principio de *accountability*: el primero, es cumplir con la legislación y los estándares internacionales que exigen mecanismos internos de protección de datos personales, y, el segundo, las herramientas tecnológicas permitirán probar y corroborar si efectivamente el programa tiene efectos en la práctica y cumple los requerimientos.

Finalmente, y no menos importante, es vital considerar la realización de un análisis de riesgos que permita detectar posibles fallas y de esta forma mitigarlos. Las amenazas o

vulneraciones pueden presentarse en cualquier momento. Una organización responsable con su estructura de protección de datos personales considera estudiar estos asuntos y plantear posibles soluciones para cumplir con lo requerido en caso de filtraciones o amenazas.

Como parte del desarrollo de derecho preventivo, se deben tomar las medidas necesarias para cumplir con lo establecido por el principio de *accountability*. Ello les permite a las organizaciones ser responsables frente a los datos, cumplir con los organismos que regulan los temas relacionados con esta materia y evitar fuertes multas y sanciones por el incumplimiento frente a las normas y regulaciones del derecho fundamental de hábeas data.

CONCLUSIONES

Las nuevas tecnologías han creado cambios en relación con la recolección y tratamiento de datos personales, fundamentalmente como consecuencia del surgimiento de negocios digitales. Por lo tanto, es importante que las empresas consideren elaborar marcos jurídicos y planes de gestión y protección de datos personales que se ajusten a estos nuevos modelos de negocio y que puedan demostrar estrategias y medidas afines, tanto en el ámbito interno como en la práctica. Las políticas y medidas deben demostrar una eficacia real y efectiva que permita determinar su aplicabilidad.

El principio de *accountability* impone la carga de proteger la información privada de las personas naturales a las organizaciones. De esta manera, es necesario que cumplan con esta carga, lo cual les va a permitir cumplir con la normativa que se exige tanto a nivel nacional como internacional.

Para lograr este objetivo, es necesario incluir programas integrales de gestión de datos personales que combinen medidas de tipo jurídico y herramientas tecnológicas que puedan servir de apoyo al empresario, al momento de estructurar marcos legales de gestión y tratamiento de datos personales. Un sistema híbrido permite cumplir con la normativa y determina que una empresa es responsable frente al uso y tratamiento de datos personales de sus consumidores.

Al realizar un análisis del principio de *accountability*, la recomendación para las empresas u organizaciones es estructurar un sistema mixto de *compliance* que combine políticas de tipo jurídico y herramientas tecnológicas para gestión e implementación de este principio en las organizaciones que realicen actividades de comercio electrónico.

Las recomendaciones en materia jurídica están orientadas a realizar un análisis de riesgos que permitan determinar cuáles son las necesidades que demanda la empresa u organización, al momento de estructurar un plan integral de gestión de datos personales. Estos requisitos, se cumplen al momento de determinar los soportes jurídicos de la recolección y tratamiento de datos personales que obedecen la normativa requerida en esta materia.

Para lograr lo anterior, es posible contar con herramientas tecnológicas como el sistema de cifrado de datos, un cuadro de mando como el BSC, un SGSDP y el *blockchain*, entre otras, que permiten una gestión adecuada de los datos y representan protección de estos frente a las amenazas externas.

Si bien es cierto que las organizaciones están expuestas a vulnerabilidades, como amenazas en los sistemas internos, la tecnología puede brindar herramientas que permiten minimizar al máximo esas posibles amenazas, que ponen en riesgo tanto los datos personales de los consumidores de comercio electrónico y, además, pueden afectar la reputación tanto digital como en el mercado concurrencial, y dado que estas empresas son competitivas pero se destacan por ser innovadoras y cumplen con los estándares que les exigen las normas. Todo esto, con el objetivo de crear conciencia en las organizaciones para evitar multas y sanciones, y cumplir con las bases de un derecho preventivo empresarial.

BIBLIOGRAFÍA

ABRAMS Martin; ABRAMS John; CULLEN Peter; GOLDSTEIN Lynn. Apéndice. "Enhanced Accountability Elements for Artificial Intelligence (AI) and Machine Learning that Directly Impacts People" The Information Accountability Foundation: Artificial Intelligence, Ethics and Enhanced Data Stewardship. 20 de septiembre de 2017. P 18.

AGENCIA EFE. El Reino Unido multa a Facebook por el escándalo de Cambridge-Analytica. [En línea] En: Agencia EFE. Octubre de 2018. Disponible en: https://www.efe.com/efe/america/portada/el-reino-unido-multa-a-facebook-por-escandalo-de-cambridge-analytica/20000064-3792293

BARRERA D. Ernesto, "Modelos de Negocios en Internet", en Internet, Comercio Electrónico & Telecomunicaciones, Bogotá. GECTI, Universidad de los Andes, Editorial Legis, 2002, pp. 216-217.

BRUNET NAHABETIÁN Laura. Protección de datos y gestión documental: Decálogo ampliado para la sociedad de la información. Rev.Fac.Der n.º 39 Montevideo July 2015. Versión en línea: ISSN 2301-0665 p. 204.

CANO MARTÍNEZ Jeimy. 2016. ¿Eres una empresa digitalmente responsable? Enero 20. [En línea] [Consultado el 14 de agosto de 2019] Disponibilidad y acceso en: https://www.linkedin.com/pulse/eres-una-empresa-digitalmente-responsable-jeimycano-ph-d-cfe.

CASTAÑO PELÁEZ Adrián. ¿Qué es la revolución digital? En: Nueva Sociedad. Revista latinoamericana de ciencias sociales. (2016)

CASTELLS Manuel. La galaxia internet. Barcelona: Areté, 2001, P 316.

Centre for Information Policy Leadership. Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance. A Discussion Document. [PDF] February 2013. P 1.

Centre For Information Policy Leadership. Who we are. Disponible en: https://www.informationpolicycentre.com/about.html

CHIAVETTA Ryan. Solution helps developers embed privacy into applications. [En línea] En: IAPP. 15 de agosto de 2019. Consultado el 25 de agosto de 2019. Disponible en: https://iapp.org/news/a/solution-helps-developers-embed-privacy-into-applications/

COOPER Tim, SIU Jade, WEI Kuangy. Corporate Digital Responsibility. Doing well by doing good. Citado por: Cano Martínez Jeimy. ¿Eres una empresa digitalmente responsable? 2016
Cooper Tim, Siu Jade, Wei Kuangy. Corporate Digital Responsibility. Doing well by doing good [PDF] En: Outlook The online journal of high-performance business. p 3.

CRESPI SERRANO Albert y CAÑABATE CARMONA Antonio. ¿Qué es la sociedad de la información? 2010 P 7.

DARK Patterns. Disponible en: https://www.darkpatterns.org/

DOMÍNGUEZ GARRIGA, Ana. Motores de Búsqueda, Redes Sociales, Rastro Digital y Publicidad Comportamental. En: Nuevos Retos para la Protección de Datos Personales en la Era del *Big Data* y de la computación ubicua. Editorial DYKINSON, S.L. Meléndez Valdés, 61-28015 Madrid. 2015. PP 36 y 37.

DZIAK Mark. Balanced scorecard (BSC). Salem Press Encyclopedia, 2018.

ESPINOSA ALONSO Carles. La información en la red y el principio de neutralidad tecnológica: la libertad de expresión y la difusión de información administrativa. En: Revista Vasca de Administración Pública n.º 81, 2009 p 87.

FINANZAS.COM Google: Aunque los datos son el nuevo petróleo, la clave es saber activarlos. [En línea] Finanzas.com 25/06/2019. Consultado el 25 de agosto de 2019 Disponibilidad en: http://www.finanzas.com/noticias/empresas/20190625/google-aunque-datos-nuevo-4020859.html

Getting Accountability Right with a Privacy Management Program. p 3. Disponible en: https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf Materiales preparados por las oficinas del Comisionado de Privacidad de Canadá y el Comisionado de Privacidad e Información de British Columbia.

GIMÉNEZ August Corrons; IBÁÑEZ, Marta Gil. ¿Es la tecnología blockchain compatible con la economía social y solidaria? Hacia un nuevo paradigma. CIRIEC-España, revista de economía pública, social y cooperativa, 2019, n.º 95, p. 191-215 y p 201.

GRAEME Codrington. The Best Ever Explanation of The Fourth Industrial Revolution. Consultado el 9 de septiembre de 2019. Disponible en https://youtu.be/okXk4Bnz2Lc

GREMMEL Robin, Los principales casos de robo de datos personales. [En línea] En: El Espectador. 15 de mayo de 2018. [Consultado el 9 de septiembre de 2019]

IFAI Transparencia y Privacidad. Guía para implementar un sistema de gestión de seguridad de datos personales. Marzo 2014. P 4.

INTERNATIONAL FINANCE CORPORATION. WORLD BANK GROUP. Blockchain: Opportunities for Private Enterprises in Emerging Markets. January 2019. P 14.

LARDINOIS Frederic. Google Proposes new privacy and anti-fingerprinting controls for the web. [En línea] En: Techcrunch. 22 de agosto de 2019. Consultado el 25 de agosto de 2019. Disponibilidad: https://techcrunch.com/2019/08/22/google-proposes-new-privacy-and-anti-fingerprinting-controls-for-the-web/

MCQUAY Terry. The Privacy Office Guide to Demonstrating Accountability. p 1. [PDF] Copyright © 2014 by Nymity Inc

MORALES NEIRA Mónica Lizet. Notas sobre el caso de Facebook y Cambridge Analytica: modelos de negocio que se basan en la explotación de datos personales. [Página Web] Innovación y Emprendimiento. Abril de 2018. [Consultado el: 18 de agosto de 2019] Disponible en: https://propintel.uexternado.edu.co/notas-sobre-el-caso-de-facebook-y-cambridge-analytica-modelos-de-negocio-que-se-basan-en-la-explotacion-de-datos-personales/

NAMÉN J. (2009). La obligación de información en las diferentes fases de la relación del consumo. p. 1.

NOSOTROS. © 2002-2017 Nymity Inc. All Rights Reserved. Consultado el: 17 de agosto de 2019. Disponible en Internet: https://latam.nymity.com/nosotros.aspx

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. PIPEDA in brief. [Página Web] [Consultado el 12 de agosto de 2019] Disponible en Internet: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. PIPEDA. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ [Consultado el 9 de septiembre de 2019.

OFFICE OF THE PRIVATE COMMISSIONER OF CANADÁ Cat. n.º IP54-58/2016ISBN 978-0-660-06541-0 Disponible en [PDF] 2015.

OFFICE OF THE PRIVATE COMMISSIONER OF CANADÁ. A guide for businesses and organizations. Privacy Toolkit. Canada´s Personal Information Act. Disponible en [PDF] Cat. n.º IP54-58/2016 ISBN 978-0-660-06541-0. Diciembre de 2015. p 12. Consultado el: 14 de agosto de 2019

OVIEDO ALBÁN Jorge. Consumidores. (PDF) En: Dikaíon -Lo Justo- Noviembre de 2006, Año 20 No 15- Chía-Colombia p 483. Consultado el: 18 de julio de 2019.

PEÑA VALENZUELA Daniel. Dos décadas de la Ley de Comercio Electrónico en Colombia [en línea] Bogotá. 22 de julio de 2019. [Consultado el: 22 de julio de 2019].

PEÑA VALENZUELA Daniel. Tecnologías de la información y derecho del consumo-Tendencias y perplejidades. En: Contexto. Revista de derecho y economía No 19 (2004) P. 1.

PÉREZ LUÑO A. E., Derechos humanos..., cit., nota 19, p. 345. Citado por: GARCÍA GONZÁLEZ Aristeo. La Protección De Datos Personales: Derecho Fundamental Del Siglo XXI. Un Estudio Comparado. Boletín Mexicano de Derecho Comparado, nueva serie, año XL, núm. 120, septiembre-diciembre de 2007. P 751.

PERFIL DE LINKEDIN: The Information Accountability Foundation. Consultado el 23 de abril de 2019. Disponible en Internet: https://co.linkedin.com/company/the-information-accountability-foundation

POLANCO LÓPEZ Hugo Armando. Manifestaciones del principio de equivalencia funcional y no discriminación en el ordenamiento jurídico colombiano. Revista Criterio Jurídico. Santiago de Cali 2016 ISSN 1657-3978 p. 43.

RAPPI. Términos y condiciones de uso de la Plataforma “RAPPI”. [En línea] Legal.Rappi.Com [Fecha de Consulta: 23 de agosto de 2019] Disponible en: https://legal.rappi.com/colombia/terminos-y-condiciones-de-uso-de-plataforma-rappi-2/?_ga=2.212683730.718552052.1566567140-410606911.1566567140

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS. Grupo de Trabajo temporal sobre autorregulación y protección de datos personales. Mayo 5 de 2006. Citado por: COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 83882 de 2018. p 16.

REMOLINA ANGARITA Nelson. La protección del consumidor en el comercio electrónico.https://www.ambitojuridico.com/noticias/columnista-impreso/mercantil-propiedad-intelectual-y-arbitraje/la-proteccion-del consultado el 11 de febrero de 2019.

REMOLINA ANGARITA Nelson. ÁLVAREZ ZULUAGA Luisa Fernanda. (2018). Guía GECTI para la implementación del principio de responsabilidad demostrada –accountability– en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos. Universidad de los Andes (Bogotá, Colombia). Facultad de Derecho. GECTI, 1-58. P 10.

REMOLINA ANGARITA Nelson. Los datos personales como motor de los negocios. En: Tratamiento de datos personales. Aproximación internacional y comentarios de la Ley 1581 de 2012. Colombia. Editorial Legis, 2013. P 8.

RODRÍGUEZ Gladys Stella. Riesgos del consumidor de comercio electrónico en las prácticas publicitarias. Revista de Derecho n.º 37, Barranquilla, 2012ISSN: 0121-869 p. 268. Disponible en [PDF].

SCHWARTZ Paul. “Data Protection Law and the Ethical Use of Analytics. Citado por: Centre for Information Policy Leadership. Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance. A Discussion Document. February 2013.

SMART LAW. Algorithmic Accountability Act: así se está regulando el futuro del *big data* y los algoritmos en Estados Unidos. [En línea] En: The Technolawgist. junio 3, 2019. Consultado el 25 de agosto de 2019. Disponible en: http://www.thetechnolawgist.com/2019/06/03/algorithmic-accountability-act-regulando-el-futuro-big-data-los-algoritmos-estados-unidos/

SMART LAW. DETOUR Act: la revolución del uso de la tecnología en los próximos años [En línea] En: The Technolawgist. junio 4, 2019. Consultado el 25 de agosto de 2019. Disponible en: http://www.thetechnolawgist.com/2019/06/04/detour-act-revolucion-us-de-la-tecnologia-en-los-proximos-anos/

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability). [PDF] 2016. P 4 [Consultado el 12 de agosto de 2019].

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Objetivos y funciones [en línea] Consultado el 12 de agosto de 2019. Disponible en Internet: http://www.sic.gov.co/objetivos-y-funciones

TAPIA, Verónica. La emergente cuarta revolución industrial, Internet de las Cosas. UTCIENCIA, [S.l.], v. 1, n. 1, PP 2,3 june 2017.

The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, Centre for Information Policy Leadership 23 de julio de 2018. Disponible en: [PDF] p 3.

The Centre for Information Policy Leadership Hunton & Williams LLP. Accountability: A Compendium for Stakeholders. Marzo de 2011. Data Protection Accountability: The Essential Elements A Document for Discussion October 2009. Prepared by the Centre for Information Policy Leadership 1 as Secretariat to the Galway Project. p 1.

THE INFORMATION ACCOUNTABILITY FOUNDATION. Consultado el 8 de septiembre de 2019. Disponible en: http://informationaccountability.org

THE INFORMATION ACCOUNTABILITY FOUNDATION. Data Stewardship Elements. January 2019. Consultado el: 3 de mayo de 2019. p 2.

THE INFORMATION ACCOUNTABILITY FOUNDATION: THE GLOBAL INFORMATION ACCOUNTABILITY PROJECT: THE FIRST FIVE YEARS. 22 de mayo de 2014. p 4.

UNIVERSIDAD SERGIO ARBOLEDA. En la Sergio. ¿Qué es Blockchain y por qué es el futuro de la seguridad de datos? Disponible en: https://www.usergioarboleda.edu.co/noticias/blockchain-la-seguridad-datos/

VIRTRU. Virtru Developer Hub. [Consultado el 25 de agosto de 2019] Disponible en: https://www.virtru.com/data-encryption-sdk/

VIRTRU. Why Virtu. [Consultado el 25 de agosto de 2019] Gartner, Predicts 2019: The Ambiguous Future of Privacy, Bart Willemsen, Daryl Plummer, *et al*., 14 November 2018. Disponible en: https://www.virtru.com/about/