TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES EN LATINOAMÉRICA

INTERNATIONAL TRANSFER OF PERSONAL DATA IN LATIN AMERICA

TRANSFERENCIA INTERNACIONAL DE DADOS PESSOAIS NA AMÉRICA LATINA

*Christian Razza**

Recibido: 05/05/2020
Aprobado: 05/06/2020

Resumen

Los datos personales se han tornado a nivel internacional un activo intangible que permite la productividad y competitividad. Por esta razón, es necesario que se regule adecuadamente su tratamiento por medio de una serie de mecanismos, derechos y principios que garanticen el derecho a la protección de datos personales. En Latinoamérica, varios países lo han reconocido constitucionalmente, sin embargo, hasta ahora no se han brindado las garantías suficientes para efectivizar su protección. Aún más grave, en ciertos países no existe regulación respecto a la transferencia internacional de datos personales (TIDP). El presente trabajo abordará el problema de que Latinoamérica no cuenta con un nivel de protección que logre garantizar seguridad y regular adecuadamente la TIDP.

Palabras clave: Privacidad; Protección; Tratamiento; Estándares; Derecho; Garantías; Dato

Summary

On an international level, personal data has become an intangible asset that enables productivity and competitiveness. For this reason, it has been necessary for its treatment to be properly regulated by a series of mechanisms, rights and principles that guarantee the right to the protection of personal data. In Latin America, several countries have recognized constitutionally, however, until now, sufficient guarantees have not been provided to make their protection effective. Even more serious, in certain countries there is no regulation regarding the international transfer of personal data (ITPD). This document raises the problem that Latin America does not have a level of protection that guarantee security and properly regulate the ITPD.

Key words: Privacy; Protection; Treatment; Standards; Right; Guarantee; Data

Resumo

Os dados pessoais passaram a fazer parte de um ativo intangível a nível internacional que permite a produtividade e a competitividade. Por esta razão, é necessário que se regule adequadamente seu tratamento por uma série de mecanismos, direitos e princípios que garantam o direito a proteção de dados pessoais. Na América Latina, vários países os reconhecem constitucionalmente, mas, até agora não se outorgaram as garantias suficientes para tornar efetiva sua proteção. Ainda mais grave, em alguns países não existe regulamentação sobre a transferência internacional de dados pessoais (TIDP). O presente trabalho abordará o problema de que na América Latina não existe um nível de proteção que outorgue a garantia de segurança e a regulamentação adequada da TIDP.

Palavras chave: Privacidade; Proteção; Tratamento; Premissas; Direito; Garantias; Dado

* Abogado por la Universidad de las Américas. Máster en Propiedad Intelectual y Nuevas Tecnologías en la Universidad Internacional de la Rioja (cursando). Consultor en derecho de competencia, laboral, societario, contractual y en nuevas tecnologías, con experiencia en protección de datos y concentraciones económicas. Actualmente, abogado en la Superintendencia de Control de Poder del Mercado.

INTRODUCCIÓN

El incremento de empresas cuyo modelo de negocios se centran en el uso de plataformas digitales durante los últimos años ha sido un fenómeno global que, por un lado, podría llevar al resquebrajamiento de algunos paradigmas del derecho de la competencia y por otro, al aprovechamiento y uso inadecuado de datos personales. Casos como Cambridge Analytica y las investigaciones que se encuentran en curso en Alemania (*Bundeskartellamt*) contra Facebook, en la Unión Europea (UE) con escudo de privacidad UE-Estados Unidos y el Congreso de los Estados Unidos contra Amazon, Facebook, Google y Apple, nos ha hecho reflexionar sobre la importancia que tienen los datos personales en la sociedad actual, pues, es un hecho que la información personal ha permitido construir empresas de miles de millones de dólares.

Los datos personales se han vuelto a nivel internacional un activo intangible que permite la productividad y competitividad. Razón por la cual se ha visto necesario que se regule adecuadamente su tratamiento por una serie de mecanismos, derechos y principios que garanticen el derecho a la protección de datos personales. El tratamiento de datos personales (TDP) debe estar concebido para servir a la humanidad, de ahí que, dentro del Reglamento General de Protección de Datos (por sus siglas en inglés GDPR) de la UE, en el considerando 4, no se concibe al derecho a la protección de datos personales como un derecho absoluto, sino en relación con su función en la sociedad y para mantener el equilibrio con otros derechos.

En Latinoamérica, varios países han reconocido el derecho a la protección de datos personales constitucionalmente, sin embargo, hasta ahora no se han brindado las garantías suficientes para efectivizar su protección. Aún más grave, en ciertos países no existe regulación respecto a la transferencia internacional de datos personales (TIDP), motivo por el cual, si los datos personales de sus ciudadanos son objeto de una de estas transferencias se encontrarían en un total estado de desprotección. La situación anterior, no solo dificulta a los países latinoamericanos su relación con dos de sus más importantes aliados comerciales, Estados Unidos y la UE, sino que además «[...] acentúa las diferencias conceptuales entre los diversos sistemas de derechos humanos, cuya característica fundamental debe residir precisamente en su universalidad» (Maqueo, Moreno y Recio 2017, 93). Históricamente, algunas legislaciones han mostrado una gran preocupación por la protección de datos personales, como es el caso de la UE que, en el 2016, con el GDPR estableció un conjunto de mecanismos para la TIDP. Por esta razón, en la UE se exige un nivel adecuado de protección a terceros países u organizaciones internacionales, a efectos de autorizar una transferencia internacional de datos. Tendencia que se ha seguido a nivel mundial: en EE.UU. con el *Privacy Shield*, la *California Consumer Privacy Act* (CCPA) y la *Stop Hacks and Improve Electronic Data Security Act* (SHIELD); y, en Latinoamérica, con la adopción y aplicación de estándares internacionales en sus legislaciones específicas sobre protección de datos personales.

En el presente trabajo se pretende evidenciar que Latinoamérica no cuenta con un nivel de protección que logre garantizar seguridad y regular adecuadamente TIDP. Para efectos de esta investigación se mencionarán los marcos regulatorios de Argentina, México y Ecuador.

PROTECCIÓN, TRATAMIENTO Y TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

En nuestra época, los avances tecnológicos se han fundido con nuestro diario vivir y prácticamente todas las áreas de la sociedad se ven afectadas por la tecnología. Este panorama ha permitido que el tráfico de información se realice rápidamente y en grandes cantidades; de suerte que, en ocasiones, se constituye

en una herramienta para facilitar el comercio y el desarrollo de las sociedades y, otras veces, en un riesgo para los derechos de las personas (Rebollo y Serrano 2017, 21-3).

Las economías digitales se han convertido en objeto de un sin número de estudios, conferencias, publicaciones, debates legislativos y comentarios de todas las personas. Desde este punto de vista, nos hemos podido dar cuenta de que nuestros datos personales, primero, han sido utilizados para fines que nunca habríamos imaginado y, luego, se han transferido entre cientos de empresas a nivel mundial. En este sentido, también nos dimos cuenta de que las autoridades no han tomado las decisiones apropiadas para evitar que el uso de datos vulnere derechos y concentre poder en manos de unos pocos.

Ahora bien, para luchar contra estos abusos, es necesario que las diferentes ramas del derecho, como el derecho de competencia y el derecho a la protección de datos personales, colaboren; ya vimos que existe una relación y un apoyo entre las agencias de control de cada una de estas ramas, por ej., en el caso de la *Bundeskartellamt* contra Facebook y, al parecer, este es el camino correcto que debemos tomar. El uso de datos sin control, sin normas que impongan límites y principios a seguir, puede, como ha sido noticia, afectar hasta a una elección presidencial. No obstante, para entender mejor qué medidas se deben tomar para proteger los datos personales, empezaremos con los elementos básicos del tema.

1. Datos personales y protección de datos personales

Los datos personales pueden ser tan sencillos como los nombres y apellidos, tan complejos como los datos biométricos, o tan sensibles como los relacionados con la salud. Los datos personales son una lista extensa y abierta que va creciendo, como el número de seguro social, los datos genéticos y hasta nuestros *likes* en Facebook. En realidad, hay miles de formas en las que nuestro propio día a día nos hace identificables (Gil 2016, 45). En este sentido, un dato personal, a simples rasgos es la información que permite identificar concretamente a una persona; específicamente, las Directrices sobre Protección de la Privacidad y Flujo Transfronterizo de Datos Personales de la Organización para la Cooperación y el Desarrollo Económico (OCDE) definen al dato personal como «[...] toda información relativa a un individuo identificado o identificable.».

Al respecto, el Tribunal Europeo de Derechos Humanos, al resolver los casos Leander vs. Suecia (1987), Z vs. Finlandia (1997) y Amann vs. Suiza (2000), señaló que los datos personales son «[...] cualquier información relativa a un individuo identificado o identificable», concepto que el Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE en el Dictamen número 4/2007 y el GDPR en su artículo 4, punto 1 acogen en su definición de dato personal.

La protección de datos personales surge en la década de los años setenta a través del desarrollo tanto legislativo como jurisprudencial de dos sistemas legales contrapuestos, el norteamericano y el europeo (Zaballos 2013, 88). Sus respectivas doctrinas son las bases más relevantes para el desarrollo de la protección de datos personales en todo el mundo.

En estados Unidos, la protección de datos personales, en sus inicios se fundamentó en el derecho a la privacidad, que tiene como origen la doctrina de *Privacy Law* desarrollada por Samuel Warren y Louis Brandeis en 1890. En Europa, en cambio, las ideas norteamericanas fueron sustituidas por la doctrina de la autodeterminación informativa, que consiste en el derecho de cada persona a determinar en qué medida puede comunicar a otros sus datos personales, idea creada por Alan Westin en 1967 (Lucena 2012, 129).

2. Configuración del derecho fundamental a la protección de datos personales

La protección de los derechos fundamentales ha variado a lo largo del tiempo, y no siempre se ha concedido el mismo nivel de protección ni se han reconocido los mismos derechos fundamentales. La Corte Constitucional de Colombia, en la sentencia C-748/11, explica que el derecho a la protección de datos personales partió como una garantía a la vida privada, que luego pasó a ser entendida como el

derecho a la autodeterminación informativa y, finalmente, como un derecho autónomo.

El derecho fundamental a la protección de datos personales comprende un conjunto de derechos que la persona puede ejercer frente a quienes sean poseedores de bases de datos públicos o privados, para conocer el contenido, uso y destino de su información (Guzmán 2013, 114). Asimismo, este derecho tiene un carácter instrumental frente a otros derechos reconocidos. Por un lado, porque el uso indebido de datos personales puede afectar otros derechos, como el de educación o salud; y, por otro, ya que permite a la persona el mantenimiento y desarrollo de su individualidad, la protección de sus derechos, bienes personales, sociales, familiares y patrimoniales (Puccinelli 1999, 68). Por consiguiente, se lo concibe como un mecanismo jurídico que otorga a la persona el control y disposición de todos sus datos (Sanz 2008, 139).

De igual manera, el derecho a la protección de datos personales es un derecho autónomo, pues protege datos de carácter personal de todo tipo y no solo los relativos al ámbito más íntimo de la vida privada. Pero también es un derecho de carácter instrumental; porque, a través de él se garantiza a las personas el pleno ejercicio de varios de sus derechos fundamentales, como el acceso a la educación, vivienda, crédito, entre otros (Villalba 2017, 38). En definitiva, su contenido conlleva una pluralidad de derechos básicos, principios y garantías que lo convierte en un derecho complejo (Valverde 2013, 21).

En este sentido, para que el ejercicio de este derecho sea efectivo, a través de él se debe poder tener acceso, actualizar, rectificar y eliminar mis datos, así como poder oponerse a su tratamiento. De aquí resultan los llamados derechos ARCO, necesarios para un adecuado tratamiento de datos a los que luego, con el GDPR, se suman el derecho a la portabilidad de los datos, la limitación del tratamiento y el derecho al olvido. Ahora, todos ellos en conjunto se denominan derechos AROLPOD. Estas garantías y derechos, en los últimos años se han visto vulnerados. Primero, porque la disparidad existente en la regulación de protección de datos entre países ocasiona una incertidumbre; dado que, debido a las plataformas digitales, las personas interactúan a nivel global y, así, sus datos también se transfieren a distintos puntos del planeta. Segundo, porque ciertos países, como es el caso de Ecuador, no cuentan todavía con una ley de protección de datos personales.

Uno de los casos más recientes e importantes es el de la agencia de competencia de Alemania**,** que impuso a Facebook restricciones de largo alcance en el procesamiento de datos de los usuarios, pues acusa a Facebook de no solo recopilar datos personales que surgen al usar la red social, sino que también reúne datos que los usuarios dejan en WhatsApp, Instagram, Masquerade, Oculus y muchos otros servicios que también pertenecen a Facebook (Bundeskartellamt 2019, 7-8), ocasionando a los usuarios de esta red social una afectación a su autonomía personal y la protección de su derecho a la autodeterminación informativa, que también está protegida por el GDPR. En el contexto de los grandes obstáculos para el cambio que existen para los usuarios de la red (efectos de bloqueo), también representa una explotación de los usuarios que es relevante según la ley antimonopolio, porque la competencia ya no es efectiva debido a la posición dominante de Facebook.

Ahora bien, a pesar de su alcance, el derecho a la protección de datos personales no se puede entender como ilimitado, en vista de que existen diferentes razones, por las que se pueden establecer limitaciones, por ej., las transferencias internacionales. Como bien señala Garriga (2016, 94), «[...] el ciudadano de un Estado social de Derecho no tiene un derecho absoluto e ilimitado sobre sus datos, sino que por ser parte de un conglomerado tiene que aceptar limitaciones en aras del interés superior». La realidad es que los datos son necesarios para realizar varias actividades lícitas, legítimas y de interés general o particular; por ende, el derecho a la protección de datos no es para oponerse a su tratamiento, sino para exigir uno correcto (Remolina, Tenorio y Quintero 2018, 48).

3. Principios rectores

El derecho a la protección de datos personales se garantiza mediante la previsión**,** en la ley, de una serie de mecanismos y elementos dirigidos a asegurar el

control y el dominio sobre los datos. Con el fin de preservar este derecho fundamental se necesita aplicar una serie de criterios específicos para su tratamiento (Sanz 2008, 139). En diferentes instrumentos jurídicos internacionales se han establecido una serie de principios que velan por el respeto a la protección de datos personales. Sin embargo, en el GDPR se han incluido los más importantes, los que la mayoría de las legislaciones sobre protección de datos han tomado como modelo y que, hoy en día, son la base sobre la que el derecho a la protección de datos se efectiviza.

El principio de licitud, lealtad y transparencia exige a los responsables y encargados del tratamiento de datos que solo lo podrán realizar si existe una justificación legal suficiente y que se deberá informar al titular de los datos sobre todo el procedimiento, sin engaño y de la forma en que se indicó (Mendoza 2017, 276). Por otro lado, el principio de limitación de la finalidad establece que el TDP se realizará únicamente en el ámbito de finalidades legítimas, explicitas y determinadas; y sus fines deberán estar determinados con precisión (Ortiz 2002, 134). El de proporcionalidad indica que nada más se deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

De igual forma, los demás principios de exactitud, vigencia, integridad y confidencialidad señalan que los datos deben estar completos, el tiempo por el cual se debe conservar los datos y la seguridad que se debe brindar cuando se está en su posesión. Este andamiaje se refuerza con el principio de responsabilidad proactiva, que obliga a los responsables y encargados del tratamiento a utilizar medidas apropiadas, efectivas y verificables que le permitan probar el correcto cumplimiento de las normas sobre protección de datos (Quesada 2017, 56).

4. Tratamiento de datos personales (TDP) y Transferencia internacional de datos personales (TIDP)

El TDP se ha convertido en una actividad cotidiana y de alta importancia para el Estado, las empresas y los particulares. Todos requieren de información personal para tomar y ejecutar decisiones de diversa naturaleza (económica, seguridad nacional, política, laboral, financiera, comercial, entre otros). La regulación del TDP no se opone al uso de datos sino a su eventual abuso, pues un inadecuado tratamiento de datos puede provocar una vulneración de los derechos humanos de sus titulares (Remolina et al. 2018, 48).

El Art. 4, número 2 del GDPR señala que el tratamiento de datos es:

> [...] Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

De esta definición se puede extraer que el TDP se puede dar de diferentes maneras, puede ser automatizado o no, y tiene la posibilidad de que existan 3 partes en un tratamiento de datos: 1) El interesado, que es la persona física titular de los datos personales; 2) El responsable, que es la persona física o jurídica, de naturaleza pública o privada que, solo o junto con otros, determina los fines y medios del TDP; y 3) El encargado, o es la persona física o jurídica, de naturaleza pública o privada, que lleve a cabo un TDP por cuenta del responsable del TDP. Por otro lado, De Terwangne (2009, 177) explica que**,** en los procesos de integración económica**,** existe la necesidad de exportar e importar datos personales entre las empresas privadas, las personas o las autoridades de los diferentes países. Procesos como el incremento de las relaciones comerciales internacionales y sociales hicieron necesario expedir normas sobre el tratamiento de datos que conciliaran la protección de la privacidad y su eventual transferencia internacional.

A partir del GDPR y de la sentencia Lindqvist vs. Gäta hovärtt., del Tribunal de Justicia de la Unión Europea (TJUE), una TIDP se produce cuando los datos personales que son tratados por un responsable o encargado del tratamiento de datos que se encuentra en el

Espacio Económico Europeo son enviados fuera de dicho territorio a un tercer país u organización internacional. De forma más amplia, es una transmisión realizada por cualquier medio, a través de las fronteras nacionales, de datos personales que sean objeto de un tratamiento de datos o cuando estos se reúnan con el propósito de someterlos al tratamiento que sea (Grande 2016, 59). En definitiva, una TIDP es un proceso de exportación o importación de datos personales contenidos en una base de datos ubicados en un Estado y que son enviados a otro o varios Estados.

La TIDP se puede dar por motivos muy variados, por ej.: «[...] seguridad pública, seguridad nacional, investigaciones contra el terrorismo, labores de inteligencia militar o policial, cooperación judicial, cooperación internacional en general, protección de un interés del titular del dato y controles de inmigración» (Remolina 2010, 376). La TIDP es de vital importancia tanto para el funcionamiento del mercado por su incidencia en el comercio internacional, como para el desarrollo de las actividades de un Estado.

Por las disparidades existentes entre las legislaciones nacionales sobre protección de datos, su transferencia internacional puede poner en riesgo los derechos de las personas. Sin embargo, sin estas transferencias difícilmente se podría dar el comercio mundial (Castellanos 2017, 6). Así pues, para evitar los posibles perjuicios que podría causar una TIDP a la privacidad de las personas y poder garantizar la libre circulación de datos personales, los Estados, así como las Uniones geopolíticas han establecido estándares de protección o convenios para regularlas.[1]

Para que los datos personales puedan ser objeto de TIDP a más de cumplir con los principios rectores para la protección de datos, se debe tomar en consideración los principios de continuidad de la protección y el principio de equivalencia necesarios para poder contar con un nivel adecuado de protección para la TIDP. El principio de continuidad de la protección tiene como propósito que, cuando los datos personales salgan de las fronteras de un Estado y se dirijan a un tercer país u organización, no pierdan el nivel de protección con el que contaban en el país de origen de los datos. Se busca que el nivel de protección del país exportador se garantice en el país importador.

Por otro lado, a nivel internacional, no todos los Estados ofrecen las mismas garantías en cuanto a la protección de datos personales. Por esta falta de uniformidad entre las legislaciones de los países, diferentes instrumentos jurídicos internacionales, como el GDPR, así como la legislación de Argentina o la de México, las Directrices de la OCDE y el *Privacy framework* de la APEC exigen, para autorizar una TIDP, que el país receptor de los datos cuente con un nivel de protección equivalente al que ofrece el país emisor.

El exigir un nivel adecuado de protección para autorizar una TIDP constituye el principio de equivalencia, que tiene como fin, según la sentencia del TJUE de 6 de octubre de 2015, en el caso Schrems, asunto C-362/14, garantizar: «[...] efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en el país emisor de datos personales.».

ESTÁNDARES PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Por las disparidades existentes entre las legislaciones nacionales sobre protección de datos, la TIDP puede poner en riesgo los derechos de las personas. Sin embargo, como señala Castellanos (2017, 6), sin la TIDP, difícilmente se podría dar el comercio mundial. Así pues, para evitar los posibles perjuicios que a la

1 De las definiciones expuestas, en una transferencia internacional de datos existe la participación de dos partes: el exportador de datos, definido en el Art. 4 literal e) del Decreto N°. 414/009 como «[...] la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realiza una transferencia de datos de carácter personal a un país tercero»; y, el destinatario, que, conforme el Art. 4 del GDPR, es «[...] la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comunican datos personales, se trate o no de un tercero».

privacidad de las personas podría causar una TIDP y poder garantizar la libre circulación de datos personales, los Estados, así como las Uniones geopolíticas (como la UE) han establecido estándares de protección o convenios para regular la TIDP.

1. EE.UU. de América

En EE.UU., el derecho a la protección de datos personales tiene, como antecedente principal, el derecho a la privacidad o *Right to Privacy*. Esta doctrina, construida por Louis Brandeis y Samuel Warren en 1890, aportó una reinterpretación de los precedentes en la materia ya que se comenzó a proteger la privacidad fuera del derecho a la propiedad (Saltor 2013, 275). No obstante, el sistema de protección de datos norteamericano «[...] no reconoce la protección de la privacidad mediante una legislación específica, sino que ello se efectúa a través de normativas sectoriales que, mediante la complementación de reglamentaciones y códigos de adhesión, propician un marco regulador singular» (Castellanos 2017, 14).

En EE.UU., en el siglo XX, se dictaron tres leyes que establecen los principios rectores que configuran el derecho a la privacidad en este país: la *Fredoom of Information Act* (FOIA) de 1966, la *Privacy Act* de 1974 y la *Right to Financial Privacy Act* (RFPA) de 1978. En el siglo XXI aparecieron: el *Safe Harbor* en el 2000, el *Privacy Shield* en 2016 para regular la TIDP con Europa, la *California Consumer Privacy Act* (CCPA) de 2018 y la *Stop Hacks and Improve Electronic Data Security Act* (SHIELD) de 2019, que entraron en vigor respectivamente en enero y marzo de 2020.

2. Del *Safe Harbour* al *Privacy Shield*

El *Safe Harbour* fue un conjunto de principios negociados entre Estados Unidos y la UE, para poder transferir datos personales entre estos territorios. Se constituyó como una institución jurídica que permitía a las empresas la transmisión de datos hacia sociedades en Estados Unidos y, a la vez, exigía el cumplimiento de una serie de principios, tales como: la posibilidad de oposición de los afectados, notificación a los afectados, transferencia ulterior a terceras empresas, integridad de los datos, seguridad, derecho de acceso y la aplicación de mecanismos que garanticen la resolución de conflictos y el cumplimiento de los principios (Ortega 2017, 86).

En el Anexo I de la Decisión, la UE reconoce solo a la *Federal Trade Commission* y al Departamento de Transportes como organismos jurídicos competentes en los Estados Unidos. Pero siempre con arreglo a las competencias que sus propias leyes les otorgan, de manera que el sistema de protección de datos en Estados Unidos es sectorial y no todos los organismos ni materias están incluidos en este acuerdo. Debido a estos problemas, y a pesar de que miles de empresas norteamericanas se adhirieron al acuerdo, en el año 2015, la sentencia del TJUE emitida en el caso Schrems invalidó la Decisión de la CE del año 2000, por la que se aprobaba el acuerdo de *Safe Harbour*, que era el principal marco jurídico que facultaba a las empresas y organizaciones de la UE a realizar TIDP a Estados Unidos (López 2017, 36).

En los fundamentos de hecho de la Sentencia, el señor Maximillian Schrems, de nacionalidad austriaca, que era usuario de la red *Facebook* desde 2008, presentó una reclamación ante el *Data Protection Commissioner* el 25 de junio de 2013, en la cual solicitaba que se prohibiera a *Facebook Ireland* transferir sus datos personales a Estados Unidos, toda vez que este país no garantizaba una protección suficiente de los datos personales conservados en su territorio.

Mediante la Decisión de ejecución (UE) N.º 2016/1250, de la CE, de fecha 12 de julio de 2016, se acordó el *Privacy Shield*, con el que se permitió de nuevo realizar TIDP desde la UE a los Estados Unidos sin necesidad de abordar la autorización de la entidad de control (Castellanos 2017, 26). Su contenido se compone de una serie de principios que vienen consagrados en los Anexos I y II de la Decisión, los cuales, en sentido amplio se estructuran en siete principios generales y dieciséis que los complementan.

Tanto el *Safe Harbour* como el *Privacy Shield* se concibieron como mecanismos para solucionar la ausencia de regulación en los Estados Unidos sobre el TDP y permitir la TIDP con la UE. Estos marcos regulatorios fueron su estándar de protección para realizar la

TIDP con la UE. No obstante, el *Safe Harbour*, que fue el marco regulatorio que más tiempo estuvo vigente, aunque fue acogido por miles de empresa americanas, no era de carácter obligatorio, no estaba en un rango igual que otras leyes americanas y se encontraba desactualizado; tal estatus dificultaba su aplicación y, por ende, tuvo que ser sustituido.

El *Privacy Shield*, si bien pretendía cubrir los vacíos de su antecesor presentó aún los mismos problemas, de suerte que no podía constituirse en un marco regulatorio obligatorio y así, no garantizaba que los Estados Unidos puedan ser considerado un país con un nivel adecuado de protección de datos personales. Por esta razón, el TJUE, en el asunto C-311/18 (Scherms II) declaró que la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-Estados Unidos (*Privacy Shield*) es inválida. Aunque el mismo Tribunal, en esa ocasión, también confirmó que las cláusulas contractuales estándar siguen siendo una herramienta válida para la transferencia de datos personales a procesadores establecidos en terceros países.

En cuanto a las últimas leyes promulgadas, está primero la CCPA, que es una ley de privacidad del consumidor que se aprobó en el Estado de California el 28 de junio de 2018. Desde que se encontraba como proyecto de ley ha sido descrita como el GDPR en los Estados Unidos. De hecho, esta ley es la legislación de privacidad más fuerte promulgada en cualquier Estado hasta el momento. Pues, otorga más poder a los consumidores sobre sus datos privados. Dada la presencia de gigantes tecnológicos con sede en California como Google y Facebook, se piensa que la CCPA está preparada para tener efectos de gran alcance en la privacidad de los datos personales.

Estos efectos se vieron de inmediato, pues casi simultáneamente, el Estado de Nueva York promulgó la ley SHIELD, que modifica la ley actual de notificación de violación de datos del Estado, impone una seguridad de datos más amplia y la notificación de violación de datos requisitos para las empresas, con la esperanza de garantizar una mejor protección para los residentes de Nueva York de las violaciones de datos de su información privada. Por la importancia del tema, se ha señalado que, en los próximos años, otros Estados seguirán el ejemplo de la CCPA y la SHIELD, y se apegarán cada vez más a los estándares de GPDR (Cobb 2019, 18).

3. Unión Europea

En Europa, después de la II Guerra Mundial, se sintió la necesidad y la obligación de defender los derechos humanos y, con la cooperación entre sus países, se creó la primera organización internacional en el continente: el Consejo de Europa (CE) (Cerda 2011, 347). Sobre esta base, a fin de proteger los derechos humanos y promover el Estado de Derecho, el CE adoptó el Convenio Europeo de Derechos Humanos (CEDH), en cuyo Art. 8 consta el derecho a la protección de datos personales.

La regulación sobre protección de datos personales en la UE se ha desarrollado a lo largo del tiempo con gran interés; debido a que, por la evolución de las tecnologías de la información y comunicación (TIC), se pudo realizar un intercambio inmediato de información sin límites físicos. Aquí es donde radica la importancia del derecho a la protección de datos personales, ya que permite proteger en estos intercambios de datos personales los derechos de los titulares de estos datos (Rojas 2014, 110).

En la UE, desde el «Convenio 108» para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981, se han emitido varias normas comunitarias que regulan la protección de datos personales, que prescriben una «protección equivalente» entre los países partes, y buscan una cooperación internacional a través de las autoridades locales de cada país.

De manera conjunta con la normativa comunitaria, los Estados que conforman la UE, en su legislación interna emitieron una serie de leyes que protegían en cierta manera los datos personales; por ejemplo en Alemania, la Ley de Hesse de 1970 y la Ley Federal Alemana de 1977. En Francia la Ley relativa a la informática, los ficheros y las libertades de 1978. Una de

las más significativas es la Ley Federal de Protección de Datos de Austria de 1978, donde se consagra, en el Art. 1, el derecho fundamental de todo ciudadano a la confidencialidad del tratamiento y comunicación de sus datos personales.

De la mano con la regulación normativa sobre protección de datos personales, en la UE hubo un importante desarrollo jurisprudencial. Uno de sus hitos más importantes fue la sentencia 209/83, dictada por el Tribunal Constitucional Federal Alemán el 15 de diciembre de 1983 sobre el censo de 1982. En ella, por primera vez se concibió al derecho a la protección de datos personales como un derecho autónomo e independiente del derecho a la vida privada; fue el primer paso para la construcción y desarrollo del derecho en este ámbito.

Una de las normativas más importantes fue la Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo tocante al TDP y a la libre circulación de estos datos. Los Estados miembros de la UE, a efectos de cumplir con las obligaciones que imponía este Directiva, fueron elevando progresivamente el nivel de protección de los datos personales, de forma que se produjo «[...] un efecto homogeneizador de los medios de protección y de los mecanismos para la eficacia de los derechos» (Rebollo 2008, 105).

Como resultado de este proceso, con la expedición del GDPR, la normativa de la UE en el campo de la protección de los datos se ha constituido como la más exigente del planeta (Guasch 2012, 422).

4. Reglamento General de Protección de Datos (GDPR)

En Europa el 27-IV-2016 se adoptó el Reglamento (UE) 2016/679 del Parlamento y del Consejo, con el que se derogó la Directiva 95/46/CE a fin de reformar la normativa ya existente sobre protección de datos personales y adaptarla al nuevo contexto mundial que, después del caso de *Cambridge Analytica*, cambió notablemente. Con el GDPR, la UE estableció todo un sistema de protección de datos personales que modificó reglas ya existentes, desarrolló aquellas que eran muy básicas y creó otras que eran necesarias. Esta novedad se orienta a una transición hacia una economía centralizada en los datos y la creación de un mercado único digital (Moritz y Gibello 2017, 116).

Respecto a la TIDP, con el GDPR, en la UE se estableció un conjunto de mecanismos para transferir datos a terceros países: decisiones de adecuación, normas contractuales estándar, normas corporativas vinculantes, mecanismos de certificación y códigos de conducta. En la UE, también debido al GDPR, para realizar una TIDP se requiere un nivel adecuado de protección. Razón por la cual, Latinoamérica se encuentra en los últimos años en proceso de adoptar estándares internacionales para la protección de datos personales y Estados Unidos debió implementar el *Privacy Shield* que, ahora, después de declarado invalido, tendrá que proponer algún nuevo escudo de privacidad o promulgar una ley que garantice la protección de datos.

En el GDPR existen tres vías por las cuales se puede realizar una TIDP, las cuales tienen distintos niveles de protección. La vía y el nivel más riguroso es una transferencia basada en una decisión de adecuación en que la Comisión Europea, después de una evaluación global del ordenamiento jurídico de un país, declara que cuenta con un nivel adecuado de protección.

Luego viene la transferencia mediante garantías adecuadas, el establecimiento de normas corporativas vinculantes o certificaciones y, por último, mediante casos excepcionales contemplados en el art. 49 del GDPR, tales como: por razones de interés público, celebración o ejecución de un contrato o cuando haya el interesado dado su consentimiento, siempre y cuando haya sido informado de los riesgos de la TIDP debido a la ausencia de una decisión de adecuación y de garantías adecuadas.

Estas tres vías son el estándar europeo de protección para realizar una TIDP, el cual se diferencia bastante del americano, que solo cuenta con normas corporativas vinculantes para la TIDP y que ofrecen protección a los datos de las personas.

REGULACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES EN AMÉRICA LATINA

En América Latina, la regulación del derecho a la protección de datos personales sigue un ritmo propio y tiene ciertas características que ameritan analizarse.

Recientemente, en las constituciones latinoamericanas se incorporó, como derecho autónomo, la protección de datos personales, frente a la necesidad de dar respuesta al proceso de evolución tecnológica (Ordóñez 2017, 85) y a los peligros de un uso indiscriminado e ilícito de datos por parte de las plataformas digitales. La razón es que los servicios que brindan se comercializan como gratuitos; aunque, en realidad, exigen un pago en forma de datos personales de los clientes que plataformas como *Google* y *Amazon* han usado para perjudicar a sus competidores, de forma que ponen en riesgo la información de las personas.

1. República de Argentina

En el Art. 43 de la Constitución de la República de Argentina se halla consagrado el derecho a la protección de datos personales. De este artículo se deriva la obligación de los organismos públicos de garantizar el acceso a la información, confidencialidad, supresión y rectificación de los datos personales. Pero, donde se encuentra reglamentada la protección de datos personales es en la Ley 25.336, promulgada el 4 de octubre del año 2000. En el Art. 2 de la Ley 25.336 se regula la protección de datos personales, sin hacer una distinción entre el ámbito público y privado.

En el capítulo 2 de la Ley 25.326 se establecen los principios generales en materia de protección de datos personales y las garantías que se deben dar al tratarlos. Allí destaca el principio de licitud para la formación de archivos de datos. También el principio de calidad de datos, que se traduce en que la recolección de datos no puede hacerse por medios desleales y que dichos datos deben ser ciertos y exactos, y su almacenamiento debe permitir el derecho de acceso a su titular. Además el principio de la información, en el sentido de que se debe informar a los titulares para qué serán tratados los datos y quiénes serán sus destinatarios y el principio de responsabilidad demostrada.

En Argentina, conforme el Art. 29, el órgano de control que gozara de autonomía funcional y actuara como órgano descentralizado en el ámbito del ministerio de justicia y Derechos Humanos de la Nación es la Agencia de Acceso a la Información Pública (y específicamente dependiente de esta es la Dirección Nacional de Protección de Datos Personales). Ella es la encargada de supervisar que se cumplan las disposiciones contenidas en la Ley 25.326, en la Ley de Acceso a la Información, y en la Ley del Registro.

Respecto a la transferencia internacional de datos se sigue el modelo europeo para autorizar una TIDP, que el Estado receptor de los datos cuente con un nivel adecuado de protección.

2. Estados Unidos Mexicanos

En México, recién con las reformas constitucionales del año 2007 y 2009 se protegen constitucionalmente los datos personales, se consagra explícitamente el derecho a la protección de los datos personales y se establecen los derechos ARCO como núcleo fundamental de este derecho (Da Cunha 2011, 323). En el año 2010 se adopta la Ley Federal de Protección de Datos en Posesión de los Particulares (LFPDPP), que tiene un ámbito de aplicación únicamente privado. Esta ley se basa en el marco normativo europeo, que apunta hacia la tendencia mundial de regulación jurídica de los datos personales para garantizar el derecho a la vida privada de los individuos, con respecto al TDP.

En la LFPDPP se establece una serie de principios para la protección de datos personales, como son: el de licitud, consentimiento, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. En su capítulo VI se establecen las competencias de la Autoridad reguladora, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Dentro del capítulo IV, en relación con el Reglamento de LDPDPP de 21 diciembre 2011, se regula los derechos ARCO más no los AROLPOD. En el capítulo V se desarrolla la TIDP, pero no se exige un nivel adecuado de protección, sino tan solo consentimiento del titular de los datos y enumera ciertos supuestos que no requieren consentimiento, además no desarrolla las transferencias ulteriores.

El 26 de enero de 2017 se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), con el fin de regular el ámbito público del TDP. Son sujetos obligados conforme el artículo 1, en el ámbito federal, estatal y municipal: «[...] cualquier autoridad, entidad, órgano y organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos». A los particulares, sean personas naturales o jurídicas, no se les aplica esta Ley sino la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En el capítulo I del Título segundo de la LGPDPPSO, en relación con la LDPDPP se aumenta y se desarrolla un conjunto de principios que el responsable del tratamiento debe cumplir cuando recolecta, almacena, usa, circula o realiza cualquier actividad con datos personales, como son los: principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad demostrada en el TDP. De la autoridad de protección de datos personales señala que sigue siendo el INAI. Y en cuanto a la TIDP, en el artículo 68 de la Ley aplicable a los sujetos obligados se señala que:

> [...] El responsable solo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obliguen a proteger los datos personales conforme a los principios y deberes que establece la presente Ley y las disposiciones que resulten aplicables en la materia.

Así pues, se evidencia que, para autorizar una transferencia internacional de datos se exige el cumplimiento de garantías adecuadas, además de necesitar el responsable del tratamiento, el consentimiento del titular de los datos y la obligación de comunicar al receptor de los datos personales las finalidades, conforme las cuales se tratan los datos personales frente al titular. No obstante, no se requiere un nivel adecuado de protección como en la UE con el GDPR.

3. República del Ecuador

Desde la incorporación y posterior desarrollo de las nuevas tecnologías, el Ecuador ha pasado por una revolución en el manejo de la información. La combinación de estas herramientas tecnológicas con el fenómeno de la globalización trajo consigo múltiples ventajas, por ej.: el desarrollo del comercio electrónico, la implementación de un gobierno en línea, y la virtualización de las relaciones de los ciudadanos, proveedores, consumidores y autoridades (Estrada, Estrada, Rodríguez y Tipantuña 2015, 54).

Todas estas actividades requieren de un TDP o de una TIDP, sin embargo, el Ecuador, en este contexto, no cuenta con una regulación que garantice un nivel adecuado de protección de datos personales. Este particular se evidencia porque la protección de datos personales en el país es incompleta, sectorial, contradictoria y desactualizada. De ahí que sea insuficiente para proteger adecuadamente los derechos de los titulares de datos personales y, además, inexistente respecto a la TIDP.

En el Ecuador se han presentado tres proyectos de ley para regular la protección de datos personales: el primero en el año 2010, por el asambleísta Vethowen Chica; el segundo en el año 2016, por la asambleísta Gabriela Rivadeneira; y el tercero en el año 2019, realizado por la Dirección Nacional de Registros de Datos Públicos (Dinardap) y el Ministerio de Telecomunicaciones. Este último ha realizado una ardua labor para redactar un nuevo proyecto de ley, que busca cumplir con estándares internacionales y ser aplicado a la realidad ecuatoriana. Esta propuesta, con este fin fue socializada con expertos y con la comunidad en general.

Históricamente, en el Ecuador se ha avanzado muy poco en legislación para la protección de datos personales. Recién en la Constitución Política de 1998

se hacía una pequeña referencia al derecho a la intimidad. Recién en el siglo XXI se han emitido algunas normativas que tratan de regular la protección de datos personales. Entre ellas destacan: la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos del 2002; el reconocimiento del derecho a la protección de datos personales en la Constitución del 2008; el desarrollo de la acción jurisdiccional del hábeas data en la Constitución del 2008 y en la Ley de Garantías Jurisdiccionales y Control Constitucional; y, la entrada en vigencia de la Ley del Sistema Nacional de Registro de Datos Públicos en el año 2010.

Si bien la Constitución del Ecuador reconoce el derecho a la protección de datos personales, la normativa interna, aunque regula en varios cuerpos normativos este derecho, no lo hace correctamente, es insuficiente para otorgar una adecuada protección a los titulares de los datos personales. El ordenamiento jurídico ecuatoriano regula esta materia de forma sectorial. Esta medida estaría bien si es que se lo hiciera de forma completa; sin embargo la regulación, al estar desperdigada en varios cuerpos normativos, es incompleta y en muchos casos contradictoria.

Existen algunos parámetros para el TDP de datos públicos, pero no se desarrollan todos los principios necesarios para un adecuado TDP. Así, los derechos de los titulares de los datos se pueden ejercer por el hábeas data, pero no todos, por ej., la limitación al TDP. Además, no se cuenta con una autoridad de control y no existe regulación respecto al TDP en el ámbito privado, y sobre a la TIDP.

En relación con este asunto, la normativa también está desactualizada y en muchos casos es errónea; ya que los conceptos o están mal desarrollados o ya no responden a los avances tecnológicos, como los conceptos de ficheros o de dato personal.

El Ecuador, en comparación con otros países de la región, no cuenta ni con un nivel mínimo de protección de datos personales. Como se mencionó antes, existen tres proyectos de ley sobre protección de datos que se han presentado en el país. No obstante, solo el último de ellos, el presentado en 2019, cumple con los criterios básicos que debe contener una ley de este tipo.

En general, el proyecto de ley realizado por la Dinardap y el Ministerio de Telecomunicaciones, a diferencia de los otros proyectos de ley mejora en la parte de técnica, redacción y fondo. Este proyecto tiene la influencia de normativas sobre datos personales, como el GDPR, la ley uruguaya, mexicana y española, de ahí que cuente con los cambios regulatorios que se han dado a nivel internacional. Sin embargo, aún le falta corregir errores, incluir algunas disposiciones y desarrollar ciertas figuras para lograr regular adecuadamente la protección de datos personales.

4. Comparación entre las regulaciones

Como se ha visto, el derecho a la protección de datos personales se tutela de una manera diferente a nivel mundial, aunque con una tendencia a dirigirse al modelo europeo. Además, debido a los riesgos de la TIDP, se ha marcado una predisposición de los Estados de exigir un nivel adecuado de protección de datos personales para autorizar una TIDP. Así pues, a partir del análisis realizado sobre la regulación de la protección de datos personales, corresponde efectuar una comparación centrada en los temas que son objeto de este trabajo.

Como se puede notar en la tabla 1, Estados Unidos, con el ahora inválido *Privacy Shield*, la CCPA y la SHIELD, y Argentina y México con sus legislaciones, han intentado alinearse al estándar de protección de datos personales que establece la UE con el GDPR. Se resalta la necesidad de contar con autoridades de control autónomas como la AEPD en España o la CNIL en Francia, para un correcto desarrollo de la protección de datos.

En cuanto a la TIDP, de igual manera se sigue la tendencia europea de establecer niveles de protección adecuados que permitan proteger a los titulares de los datos[2]. (véase Tabla 2)

2 Ecuador es un caso aparte, dado que no cuenta con una ley de protección de datos personales y, en las pocas leyes donde se regula algún aspecto sobre la protección de datos, no se hace mención sobre la TIDP.

Tabla 1: Aspectos generales sobre la protección de datos personales

	Argentina	México	Ecuador	EE.UU.	GDPR (UE)
Norma constitucional sobre la protección de datos	✓	✓	✓	X	—
Legislación general sobre protección de datos personales	✓	✓	X	X	✓
Normativa sectorial en cuanto al TDP	✓	X	X	✓	—
Derechos ARCO	✓	✓	✓*	X	✓
Derechos AROLPOD	X	X	X	X	✓
TDP especial para datos personales sensibles	✓	✓	X	✓	✓
Medidas de seguridad	✓	✓	X	X	✓
Autoridad de control independiente	X	✓	X	X	✓
Recursos administrativos y acciones judiciales	✓	✓	X	X	✓
Obligaciones a los responsables y encargados del TDP	✓	✓	X	✓	✓
Principios para el TDP	✓	✓	X	✓	✓
Regulación sobre la TIDP	✓	✓	X	✓	✓
Sanciones	✓	✓	X	✓	✓

Nota: comparación entre las normativas de protección de datos de países latinoamericanos y los estándares de la RIPD.
El símbolo «—» significa que no aplica.
* Por el Hábeas Data se ejercen los derechos ARCO, más no los nuevos derechos, como el de limitación al TDP.

Tabla 2: Aspectos generales respecto a la TIDP

	Argentina	México	Ecuador	GDPR	Privacy Shield
Definición sobre la TIDP	✓	X	X	X	X
Desarrollo de las TIDP ulteriores	X	X	X	✓	✓
Exigencia de un nivel adecuado para la TIDP	✓	X	X	✓	✓
Garantías adecuadas para la TIDP	X	✓	X	✓	X
Normas corporativas vinculantes para la TIDP	X	✓	X	✓	✓
Casos excepcionales para la TIDP	✓	✓	X	✓	✓
Principios propios de la TIDP	X	X	X	✓	X

Nota: comparación de los niveles de protección para realizar una TIDP

CONCLUSIONES Y RECOMENDACIONES

Desde la incorporación y posterior desarrollo de las nuevas tecnologías, Latinoamérica ha pasado por una revolución en el manejo de la información. La combinación de estas herramientas tecnológicas con el fenómeno de la globalización trajo consigo múltiples ventajas, como: el desarrollo del comercio electrónico, la implementación de un gobierno en línea, y la virtualización de las relaciones de los ciudadanos, proveedores, consumidores y autoridades. Todas estas actividades requieren de la TIDP, de ahí la necesidad de buscar armonizar las legislaciones relativas a la protección de datos personales.

A nivel internacional, por los riesgos que implica una TIDP se ha buscado una armonización de criterios respecto a su regulación, de modo que se pueda establecer un nivel mínimo de protección con el que deben contar los países para poder efectuar una TIDP. La UE y Estados Unidos son quienes más han desarrollado este tema, de forma que sus modelos de protección de datos personales son los que a nivel mundial tienen mayor preeminencia. Estados Unidos adopta un enfoque sectorial y de autorregulación que, con los últimos casos que han salido a luz, principalmente en contra de *Facebook* y *Google*, manifiesta sus falencias, mientras que la UE adopta un enfoque fundamentado en una norma general de aplicación extraterritorial, así como la exigencia de contar con autoridades de control independientes y niveles adecuados de protección que han llevado, desde la entrada en aplicación del GDPR, a multar a varias empresas.

En Latinoamérica, si bien son varios los países que regulan la protección de datos personales para proteger los derechos de sus ciudadanos, y desarrollar el comercio internacional y electrónico, aún existen ciertas falencias en la regulación. Por ejemplo, contar con una autoridad de control independiente, regular adecuadamente la TIDP, poder sancionar a los infractores con multas que puedan causar un grado de responsabilidad y actualizar las legislaciones sobre protección de datos. Falta todavía mucho para lograr la protección que brinda el GDPR, pero un paso importante es comenzar a tener una cultura de protección de nuestros datos personales. Por otro lado, debe existir una interrelación entre las agencias de competencia, defensa del consumidor y las de protección de datos, pues de esta forma se podrá controlar que las empresas y todo aquel que trate datos personales comprenda que no puede usarlos sin cumplir con las garantías y estándares básicos de protección.

La promulgación en el Ecuador de una ley de protección de datos personales permitirá regular la forma en que las empresas nacionales y extranjeras, además de los entes públicos utilizan, procesan, conservan y explotan los datos personales de las personas naturales en el Ecuador. El proyecto de ley construido por la Dinardap es la base por la cual se debe construir la ley de protección de datos, dado que su aprobación traería la oportunidad tanto de desarrollar el comercio internacional como de proteger los datos personales de sus ciudadanos. Sin perjuicio de lo anterior, se recomienda la inclusión de ciertas precisiones en el proyecto, como: precisar adecuadamente un tratamiento especial a los datos personales sensibles, establecer una autoridad de control independiente, mejorar ciertos conceptos (como dato personal), no ser repetitivo en la necesidad de consentimiento del titular de los datos, incluir los conceptos de TIDP, exportador e importador de datos, desarrollar las TIDP ulteriores y definir otra forma de cálculo para aplicar las sanciones pecuniarias y corregir los porcentajes del cálculo de estas sanciones.

BIBLIOGRAFÍA

Bundeskartellamt. 2019. "Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing". Consultado el 25-IV-2020. https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4

Castellanos Rodríguez, Albert. 2017. «El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio Privacy Shield». *ICPS Working Papers* 350: 1-34. Consultado el 15-IV-2020. https://www.icps.cat/archivos/Workingpapers/wp350.pdf?noga=1

Cerda, Alberto. 2011. «El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea». *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso 36: 327-356*. Consultado el 20-V-2019. https://scielo.conicyt.cl/pdf/rdpucv/n36/a09.pdf

Cobb, Stephen. 2019. «GDPR: ¿el primer paso hacia una ley de privacidad global?». *ESET* 1: 15-19. Consultado el 20-IV-2020. https://empresas.eset-la.com/archivos/novedades/74/Cybersecurity_Trends_2019_v6-ESP.pdf

Da Cunha, Teresa. 2011. «Las recientes reformas en materia de protección de datos personales en México». *Anuario Jurídico y Económico Escurialense* 44: 317-334. Consultado el 29-III-2020. https://webcache.googleusercontent.com/search?q=cache:QvlznE2PZ80J:https://dialnet.unirioja.es/descarga/articulo/3625376.pdf+&cd=1&hl=es&ct=clnk&gl=ec

De Terwangne, Cécile. 2009. «Is a Global Data Protection Regulatory Model Possible?». En *Reinventing data protection?*, editado por S. Gutwirth, Y. Poullet, P. De Hert, C. De Terwangne y S. Nouwt, 175-189. Dordrecht: Springer.

Estrada, José, Estrada, Juan, Rodríguez, Ana, y Tipantuña, Christian. 2015. «Ecuador y la Privacidad en Internet: Una Aproximación Inicial». *Revista Politécnica*, 1. Consultado el 28-III-2020. https://revistapolitecnica.epn.edu.ec/ojs2/index.php/revista_politecnica2/article/view/556.

Foro de Cooperación Económica Asia-Pacífico. 2004. «*Marco de privacidad de la APEC de 2004*». Consultado 18-III-2020. https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

Garriga, Ana. 2016. *Nuevos retos para la protección de datos personales en la era del Big Data y la computación ubicua*. Madrid: Dykinson.

Gibello, Valentin. y Moritz, Marcel. 2017. «El Reglamento Europeo (UE) 2016/679: análisis de un claroscuro». *Foro 27*: 115-128. Consultado el 25-III-2020. http://repositorio.uasb.edu.ec/bitstream/10644/5948/1/08-TC-Moritz-Gibello.pdf

Gil, Elena. 2016. *Big data, privacidad y protección de datos*. Madrid: Boletín Oficial del Estado.

Gobierno de México. s.f. «*Constitución Política de los Estados Unidos Mexicanos de 5 de febrero de 1917*». Consultado el 10-V-2020. http://www.sct.gob.mx/JURE/doc/cpeum.pdf

Grande, Martha. 2016. «Transferencia internacional de datos personales desde España a países iberoamericanos». *Informática y Derecho* 1: 55-70. Consultado el 10-IV-2020. https://docs.wixstatic.com/ugd/fe8db5_a143e0cda3b44d5998a5c1fe4c70c828.pdf

Guasch Portas, Vicente. 2012. «La transferencia internacional de datos de carácter personal». *Revista de Derecho UNED* 11: 413-453. Consultado el 20-IV-2020 de http://revistas.uned.es/index.php/RDUNED/article/view/11139/10667

Guzmán, María. 2013. «El derecho fundamental a la protección de datos personales en México: análisis desde la influencia del ordenamiento jurídico español». Tesis Doctoral. Universidad Complutense de Madrid. https://eprints.ucm.es/22817/1/T34727.pdf

López, Leticia. 2017. «Las transferencias de datos a EE.UU.: la transición del Safe Harbor al Privacy Shield y un paso más allá». *Actualidad jurídica Uría Menéndez* 45: 36-38. Consultado el 25-III-2020. https://www.uria.com/documentos/publicaciones/5315/documento/art03.pdf?id=6965

Lucena, Isabel. 2012. «La protección de la intimidad en la era tecnológica: hacia una reconceptualización». *Revista Internacional del Pensamiento Político 7*: 117-144. Consultado el 1-IV-2020. http://www.pensamientopolitico.org/Descargas/RIPP07117144.pdf

Maqueo, María, Moreno, Jimena, y Recio, Miguel. 2017. «Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario». *Revista de Derecho Valdivia* 1: 77-96. Consultado el 30-IV-2020. https://scielo.conicyt.cl/pdf/revider/v30n1/art04.pdf

Oficina del Asesor Jurídico de Revisión de la Cámara de Representantes de los Estados Unidos. s.f. «Right to Financial Privacy Act, 12 U.S.C. §§ 3401/342, Ley de libertad de información de 1978». Consultado el 19-IV-2020. http://uscode.house.gov/view.xhtml?path=/prelim@title12/chapter35&edition=prelim

Ordóñez, Luis. 2017. «La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración». Foro 27: 83-114. Consultado el 14-IV-2020. http://repositorio.uasb.edu.ec/bitstream/10644/5947/1/07-TC-Ordo%C3%B1ez.pdf

Organización de Estados Americanos. s.f. «Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la OCDE de 1980.» Consultado el 5-IV-2020. http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf

Ortega, Alfonso. 2017. «Transferencia Internacional de Datos de Carácter Personal: del Safe Harbour al Privacy Shield». *Lex Mercatoria*, 4: 85-90. Consultado el 25-III-2019. http://revistas.innovacionumh.es/index.php?journal=lexmercatoria&page=article&op=view&path%5B%5D=1093&path%5B%5D=208

Patterson Belknap. 2018. *California Consumer Privacy (CCPA), Ley de privacidad del consumidor de California*. Consultado el 30-IV-2020. https://www.pbwt.com/content/uploads/2018/06/California-Consumer-Privacy-Act1.pdf

Puccinelli, Oscar. 1999. *El habeas data en Indoiberoamérica*. Bogotá: Temis.

Rebollo, Lucrecio. 2008. *Vida privada y protección de datos en la Unión Europea*. Madrid: Dykinson.

Rebollo, Lucrecio. y Serrano, María. 2017. *Manual de Protección de Datos* (2a. ed.). Madrid: Dykinson.

Remolina, Nelson, Tenorio, Manuel., y Quintero, Gustavo. 2018. *De la responsabilidad demostrada en las funciones misionales de la Registraduría Nacional del Estado Civil: Hacia un programa de gestión de datos personales y la consolidación de un buen gobierno corporativo en el tratamiento de esa clase de información*. Bogotá: Temis.

Remolina, Nelson. 2010. "¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?" *Revista Colombiana de Derecho Internacional*, 16. Consultado el 15-IV-2020. https://revistas.javeriana.edu.co/index.php/internationallaw/article/view/13847

Rojas, Marcela. 2014. "Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales". *Novum Jus*, 8(1). Consultado el 19-IV-2020. https://editorial.ucatolica.edu.co/ojsucatolica/revistas_ucatolica/index.php/Juridica/article/viewFile/652/670

Saltor, Carlos. 2013. «La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina». Tesis doctoral. Universidad Complutense de Madrid. https://eprints.ucm.es/22832/1/T34731.pdf

Sanz, Lourdes. 2008. «Principios de la Protección de Datos». En *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia,* coordinador Carlos Lesmes, 138-162. Valladolid: LEX NOVA.

Valverde, Antonio. 2013. «Protección de datos de carácter personal y derechos de información de los representantes de los trabajadores». *Temas Laborales* 118: 13-54. Consultado el 6-IV-2020. http://www.juntadeandalucia.es/empleo/anexos/ccarl/33_1392_3.pdf

Villalba, Andrea. 2017. «Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa». *Foro 27*: 23-42. Consultado el 18-IV-2019. http://repositorio.uasb.edu.ec/bitstream/10644/5944/1/04-TC-Villalba.pdf

Warren, Samuel. y Brandeis, Louis. 1890. «The Right to Privacy». *Harvard Law Review* 5: 193-220. Consultado el 30-IV-2020. http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Zaballos, Emilia. 2013. «La Protección de Datos Personales en España: Evolución Normativa y Criterios de Aplicación». Tesis Doctoral. Universidad Complutense de Madrid. https://eprints.ucm.es/22849/1/T34733.pdf

Legislación y jurisprudencia

Asamblea Nacional del Ecuador. s.f. «Proyecto de Ley de Protección a la Intimidad y a los Datos Personales de 2010». Consultado el 12-IV-2020 a http://ppless.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/1f0a354a-3380-46d8-b828-f912f5dc13cf/Proyecto%20de%20Ley%20de%20Protecci%C3%B3n%20a%20la%20Intimidad%20y%20a%20los%20Datos%20Personales%20Tr.%2025508.pdf

Asamblea Nacional del Ecuador. s.f. «Proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales de 2016». Consultado el 12-IV-2020. http://ppless.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/843473d9-a8b3-4c72-8bd3-7d121aba3e66/Proyecto%20de%20Ley%20Org%C3%A1nica%20de%20la%20Protecci%C3%B3n%20de%20los%20Derechos%20a%20la%20Intimidad%20y%20Privacidad%20sobre%20los%20Datos%20Personales%20Tr.%20254848.pdf

Comisión Europea. 2007. *Dictamen no 4/2007 de 20 de junio de 2007 sobre el concepto de datos personales del Grupo de protección de las personas en lo que respecta al tratamiento de datos personales del artículo 29*. Consultado el 4-IV-2020. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

Constitución de la República del Ecuador, 2008 (Registro Oficial 449 de 20-X-2008).

Constitución Política de la República del Ecuador, 1998 (Registro Oficial 1 de 11 de agosto de 1998).

Corte Constitucional de Colombia. 2011. *Sentencia C-748/11 de la Corte Constitucional de Colombia de 6-X-2011*. Consultado el 16-IV-2020. http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

Corte Europea de Derechos Humanos. 1987. *Caso Leander vs. Suecia sentencia de 26 de marzo de 1987, asunto 9238/81 del Tribunal Europeo de Derechos Humanos, Corte Chamber*. Consultado el 13-IV-2020. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}

Corte Europea de Derechos Humanos. 1997. *Caso Z vs. Finlandia, sentencia de 25 de febrero de 1997, asunto 9/1996/627/811 del Tribunal Europeo de Derechos Humanos*. Consultado el 15-IV-2020. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58033%22]}

Corte Europea de Derechos Humanos. 2000. *Caso Amann vs. Suiza sentencia de 16 de febrero de 2000, asunto 27798/95 del Tribunal Europeo de Derechos Humanos 2000-II*. Consultado el 30-III-2020. https://hudoc.echr.coe.int/spa#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-162541%22]}

Decreto Ejecutivo 2471, de 11 de agosto de 2005, Reglamento a la Ley Orgánica de Transparencia y Consultado a la Información Pública (Registro Oficial 507 de 19-I-2005).

Decreto Ejecutivo 525, de 3-X-2018, Reglamento a la Ley Orgánica de Gestión de la Identidad y Datos Civiles (Registro Oficial 353, de 23-X-2018).

Decreto Ejecutivo 950, de 11 de marzo de 2016, Reglamento a la Ley del Sistema Nacional de Registro de Datos Públicos (Suplemento al Registro Oficial 718, de 23-III-2016).

Departamento de Justicia de los Estados Unidos. 1966. «*Freedom of information Act, 5 U.S.C. § 552ª, Ley de libertad de información de 1966*». Consultado el 27-IV-2020. https://www.justice.gov/oip/freedom-information-act-5-usc-552

Departamento de Seguridad Nacional de los Estados Unidos. 1974. «*Privacy Act, 5 U.S.C. § 552ª, Ley de Privacidad de Estados Unidos de Norteamérica de 1974*». Consultado el 12-IV-2020. https://www.uscis.gov/about-us/freedom-information-and-privacy-act-foia/privacy-act-1974

Derecho Chile. 2016. «*Sentencia 209/83 del Tribunal Constitucional Federal Alemán de 15 de diciembre de 1983, Ley del Censo*». Consultado el 17-IV-2020. http://www.derecho-chile.cl/sentencia-de-15-de-diciembre-de-1983-del-tribunal-constitucional-federal-aleman-ley-del-censo/

Dirección Nacional de Registro de Datos Públicos. 2019. «*Proyecto de la Ley Orgánica de Protección de datos Personales de 19 de septiembre de 2019*». Consultado el 30-IV-2020. https://www.dinardap.gob.ec/wp-content/uploads/downloads/2019/09/PROYECTO-LEY-DE-PROTECCION-DE-DATOS-PERSONALES.pdf

Eur-Lex. 2019. «Caso Lindqvist vs. Gäta hovärtt, sentencia de 6 de noviembre de 2003 del Tribunal de Justicia de la Unión Europea». Consultado el 15-IV-2020. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN

Eur-Lex. 2019. «Caso Schrems vs. Data Protection Commissioner, sentencia de 6-X-2015, asunto C-362/14 del Tribunal de Justicia de la Unión Europea, Gran Sala». Consultado el 18-III-2020. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62014 CJ0362&from=ES

Eur-Lex. 2019. «Decisión de ejecución, Privacy Shield UE-EE. UU 2016/1250 de la Comisión Europea de 12 de julio de 2016». Consultado el 2-V-2019. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D1250&qid=1542660556803&from=EN

Eur-Lex. 2019. «*Decisión de la Comisión 2000/520/CE, Safe Harbor Privacy Principles de la Comisión Europea de 26 de julio de 2000*». Consultado el 2-IV-2020. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000D0520&from=en

Eur-Lex. 2019. «*Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos de 1995*». Consultado el 4-IV-2020. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

Eur-Lex. 2019. «*Reglamento General de Protección de datos del Parlamento Europeo y del Consejo UE 2016/679 (GDPR) de 2016.* Consultado el 15-IV-2020. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Honorable Cámara de Diputados. s.f. «Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México de 2010». Consultado el 30-IV-2020. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Honorable Cámara de Diputados. s.f. «Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de México de 2017». Consultado el 14-IV-2020. http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Honorable Cámara de Diputados. s.f. «Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México de 2011». Consultado el 10-IV-2020. http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

Infoleg. (s.f.). «Reglamentación de la ley N°. 25.326, relativo a la protección de datos personales de Argentina de 2001, Decreto N°. 1558/2001». Consultado el 25-III-2019. http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/texact.htm

Legisalud. s.f. «Constitución de la Nación Argentina de 23 de agosto de 1994». Consultado el 10-IV-2019. http://test.e-legis-ar.msal.gov.ar/leisref/public/showAct.php?id=877

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, de 2002 (Suplemento al Registro Oficial 557 de 17-IV-2002).

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, de 2009 (Suplemento al Registro Oficial 52 de 22-X-2009).

Ley Orgánica de Gestión de la Identidad y Datos Civiles, de 2016 (Suplemento al Registro Oficial 684 de 4-II-2016).

Ley Orgánica de Transparencia y Consultado a la Información Pública, de 2004 (Registro Oficial 337 de 18-V-2004.

Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, de 2010 (Suplemento al Registro Oficial 162 de 31-III-2010).

Organización de Estados Americanos. s.f. «Ley de Protección de Datos Personales de Argentina, N°. 25.326 de 2000». Consultado el 25-III-2020. https://www.oas.org/juridico/PDFs/arg_ley25326.pdf

Tribunal Constitucional Español. s.f. «Sentencia 292/2000 del Tribunal Constitucional Español de 30 de noviembre de 2000». Consultado el 16-IV-2019. http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276#complete_resolucion&completa