Christian Razza

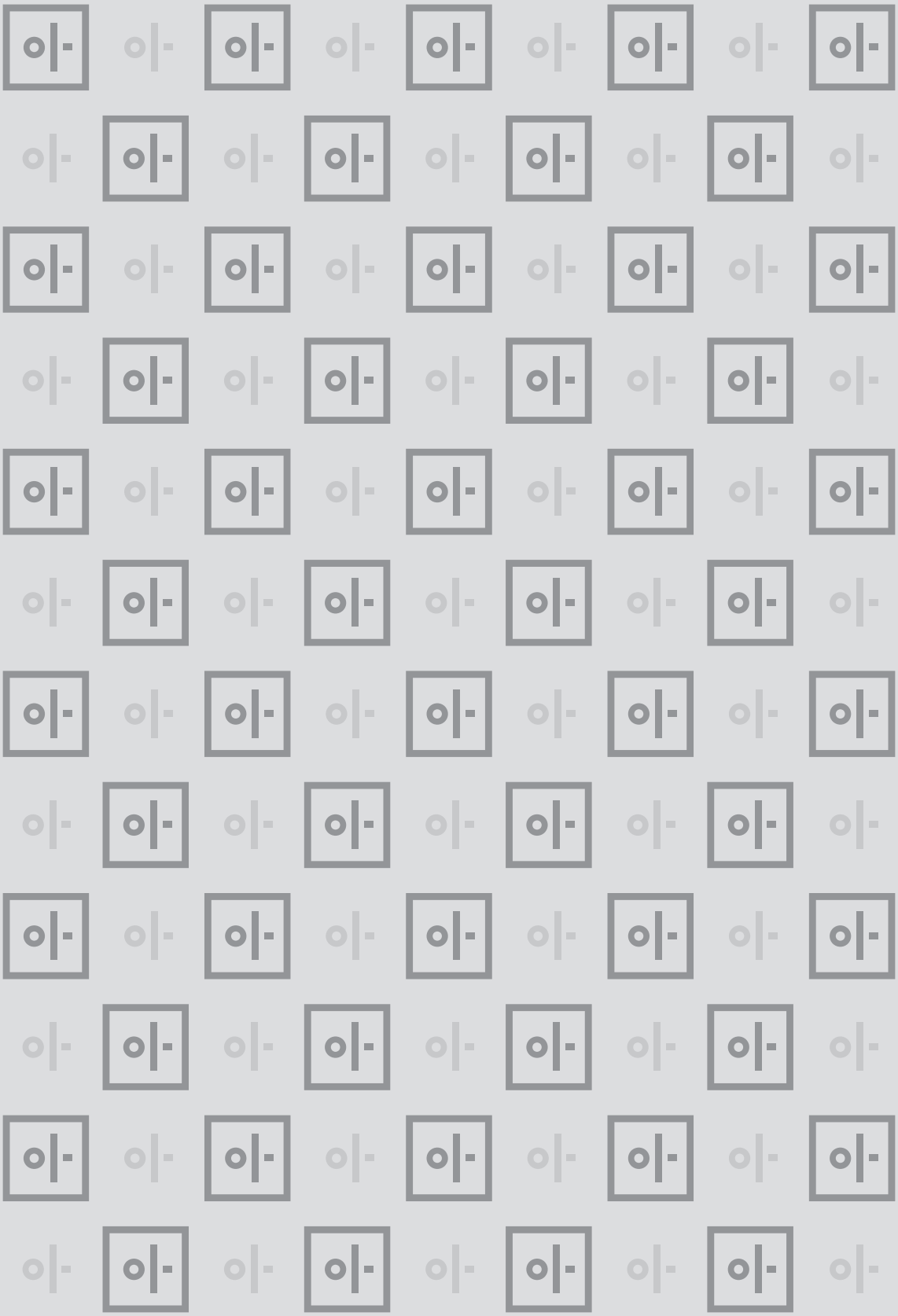
La transferencia internacional de datos personales en Ecuador

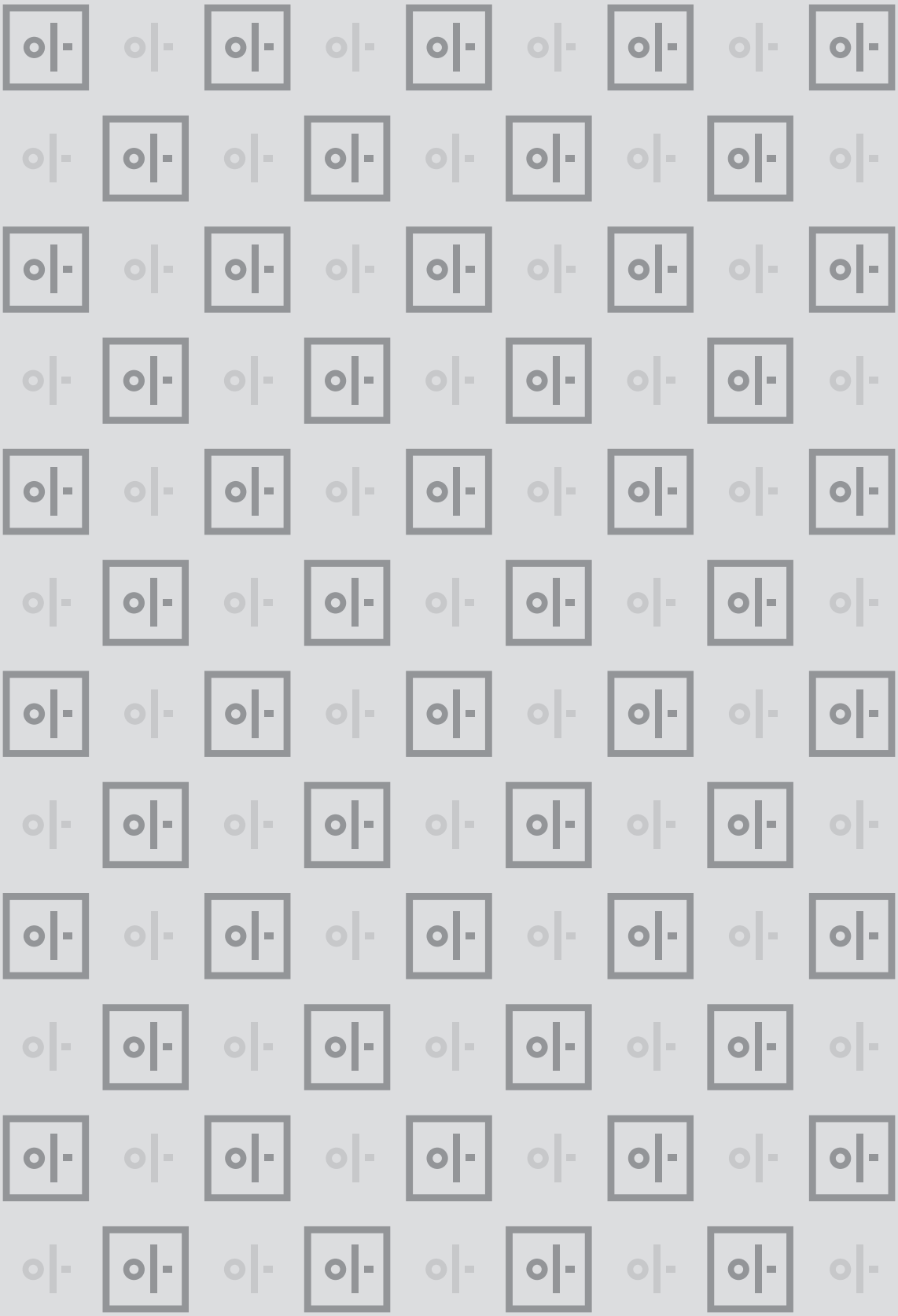
Protección frente al libre flujo

-pre | udla ediciones

Christian Alejandro Razza Sandoval

Investigador predoctoral en la Universidad de Barcelona. Abogado por la Universidad de Las Américas. Máster en Estudios Jurídicos Avanzados por la Universidad de Barcelona. Máster en Propiedad Intelectual, Competencia y Nuevas Tecnologías por la Universidad Internacional de la Rioja. Se ha desempeñado como asesor jurídico de empresas ecuatorianas y extranjeras. Ha sido abogado en importantes estudios jurídicos y en la Superintendencia de Control del Poder de Mercado. Tiene experiencia profesional en derecho administrativo, del trabajo, *compliance*, protección de datos y derecho de la competencia.





La transferencia internacional de datos personales en Ecuador

La transferencia internacional de datos personales en Ecuador

Protección frente al libre flujo

Christian Razza

La transferencia internacional de datos personales en Ecuador
Protección frente al libre flujo
© Christian Razza

© Universidad de Las Américas
Facultad de Derecho
Campus UDLA park
Redondel del Ciclista, Antigua Vía a Nayón, Quito EC 170124
www.udla.edu.ec
Quito, Ecuador

Primera edición: noviembre, 2021

EDITORA
Susana Salvador Crespo
Coordinadora Editorial UDLA

CUIDADO DE LA EDICIÓN
Fabricio Cerón Rivas
Analista editorial UDLA

CORRECCIÓN Y ESTILO
Editorial El Conejo

DISEÑO DE CUBIERTA
Editorial El Conejo

DIAGRAMACIÓN
Editorial El Conejo

ISBN: 978-9-9427-7932-8

Gracias por respetar las leyes del copyright al no reproducir, escanear ni distribuir ninguna parte de esta obra, sin la debida autorización. Al hacerlo está respetando a los autores y permitiendo que la UDLA continúe con la difusión del conocimiento.

Reservados todos los derechos. El contenido de este libro se encuentra protegido por la ley.
Previa a su publicación, esta obra fue evaluada bajo la modalidad de revisión por pares anónimos.

Contenido

Introducción, 11

Capítulo primero

Protección, tratamiento y transferencia internacional de datos, 15

El dato, 18
Datos personales, 19
Protección de datos personales, 21
Fundamento, 22
Derecho fundamental, 23
Principios rectores, 25
Tratamiento de datos personales, 28
Transferencia internacional de datos Personales, 30

Capítulo segundo

Estándares para la transferencia internacional de datos personales, 37

Estados Unidos de América, 40
Del Fredoom of Information Act al Right to Financial Privacy Act, 40
Del Safe Harbour al Privacy Shield, 43
California Consumer Privacy Act, 47
Unión Europea, 49
Antecedentes normativos, 50
General Data Protection Regulation, 54
Regulación de la protección de datos personales en América Latina, 58

República de Argentina, 58
Estados Unidos Mexicanos, 59
República Federativa del Brasil, 61
Estándar de protección de datos personales para los Estados Iberoamericanos, 62
Organizaciones internacionales que regulan la transferencia internacional de datos, 64

Capítulo tercero

Estándar adecuado de protección para la transferencia internacional de datos personales en Ecuador, 69

Situación actual de la protección de datos personales en Ecuador, 72
Propuestas de ley presentadas en Ecuador, 78
Niveles de protección adecuados para realizar una transferencia internacional de datos personales, 87
Estándar de protección adecuado para realizar una transferecia internacional de datos personales, 90

A manera de conclusión, 93

Referencias, 97

Introducción

En la época actual, las actividades sociales, culturales, económicas, jurídicas y políticas constantemente rebasan fronteras. Los avances tecnológicos se han unificado con nuestra cotidianeidad y prácticamente todas las áreas de la sociedad se ven afectadas por ello. Este panorama ha permitido que el tráfico de información se realice con rapidez y en grandes cantidades; de suerte que, unas veces, se constituye como una herramienta para facilitar el comercio y el desarrollo de las sociedades, y otras veces, es en un riesgo para los derechos de las personas (Rebollo y Serrano 2017, 21-23).

Los datos personales se han vuelto, tanto a nivel nacional como internacional, un activo intangible que permite la productividad y competitividad. Razón por la cual, es necesario regular 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 concebirse para servir a la humanidad; por eso, en el Reglamento General de Protección de Datos (por sus siglas en inglés, GDPR), de la Unión Europea (UE), en el considerando 4, no se concibe el derecho a la protección de datos personales como uno absoluto, sino en relación con su función en la sociedad, para mantener el

equilibrio con otros derechos. Además, debido al desarrollo de la tecnología y al aumento de la transferencia internacional de datos personales (TIDP), no debemos restringir sino controlar el tratamiento de estos datos.

La democratización del acceso, almacenamiento y transformación de la información es la premisa en la que se fundamentan las principales empresas del mundo, como señaló el catedrático Víctor Ayalde (2016, 137-138). Google es el filtro de contenidos e información más utilizado; Facebook masificó la posibilidad de publicar contenido social; Twitter es por excelencia la plataforma de opinión; Uber reduce muchos costos de transacción entre pasajeros y transportadores; y Airbnb permite a varios oferentes comunicarse con consumidores que antes no tenían un punto de encuentro. Y así sucesivamente en los diferentes mercados (Taskrabbit, Lending club, Splinter). Todos tienen como común denominador el acceso a más información y a la reducción de los costos de transacción entre las partes. Nadie niega los beneficios del uso de datos para las empresas y los consumidores; no obstante, por estas eficiencias, este tipo de empresas imponen condiciones comerciales desleales a sus clientes, pues vulneran sus datos personales.

En este contexto, Ecuador, como parte de la economía mundial, está expuesto a múltiples presiones, tanto políticas como económicas, las cuales se relacionan con la protección de datos personales. Por tanto, constituye un desafío para el Derecho, por una parte, la necesidad de equilibrar el interés público que puede existir respecto a estos datos, y, por otra, el velar por el respeto a los derechos fundamentales de la persona titular de dicha información. Así pues, la ausencia, por un largo tiempo, en nuestro país de una ley de protección de datos ha dificultado la relación con dos de sus más importantes aliados comerciales: Estados Unidos y la Unión Europea.

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).

En Latinoamérica, varios países han reconocido el derecho a la protección de datos personales constitucionalmente; sin embargo, hasta ahora no se han brindado garantías suficientes para efectivizar su protección. Aún más grave es el caso de Ecuador, pues hasta hace poco no existía una ley de protección de datos personales, motivo por el cual si nuestros datos hubiesen sido objeto de una de estas transferencias se encontrarían en un total estado de desprotección.

En este sentido, el problema jurídico que pretendo resolver con este trabajo se resume en la siguiente pregunta: ¿cuál es el estándar adecuado de protección con el que debería contar Ecuador para proteger nuestros datos personales? Sobre este problema jurídico, defiendo la posición de que Ecuador, para garantizar el derecho a la protección de datos personales –en el contexto de la TIDP–, requiere adoptar y aplicar un estándar de protección que recoja los principios y criterios que se han desarrollado en Europa y Estados Unidos.

De tal forma, este libro se dividie en tres capítulos. En el primero expongo los conceptos generales sobre la protección de datos personales, haciendo hincapié en su tratamiento y en la TIDP. En el segundo, me enfocó en analizar los dos principales modelos de protección para la TIDP existentes: el estadounidense y el europeo, pero añado un estudio de las principales organizaciones internacionales que han emitido regulaciones sobre la TIDP y analizo cómo estos han sido aplicados en América Latina. En el tercero, partiendo del estudio de la situación actual de Ecuador respecto a la protección de datos, determino cuál es el estándar adecuado de protección con la que el país debe contar para la TIDP y, por ende, garantizar que estas transferencias se realicen respetando los derechos y garantías establecidas en la Constitución y en los cambios regulatorios ocurridos en el derecho comparado durante los últimos años. Al final se presentan, de manera resumida, los principales resultados de la investigación.

CAPÍTULO PRIMERO

Protección, tratamiento y transferencia internacional de datos

La tecnología ha diluido la noción de fronteras territoriales, lo cual amplía el ámbito de actuación de las empresas e insta a los Estados a adaptar su legislación para estos cambios. Este nuevo contexto global, donde diariamente se intercambian datos personales, implica una problemática para el Derecho, pues debe brindar los mecanismos legales apropiados para proteger los derechos de las personas.

El tratamiento de nuestros datos, por parte de las empresas, se ha convertido en el objeto de un sinnúmero de estudios, conferencias, publicaciones, debates legislativos y comentarios de todas las personas. Así, nos hemos podido dar cuenta de que nuestros datos personales, primero, han sido utilizados para fines que nunca habríamos imaginado y, luego, que han sido transferidos entre cientos de empresas a nivel mundial. En este sentido, también consideramos que las autoridades no han tomado las decisiones apropiadas para evitar que el uso de datos vulnere derechos y concentre poder en las manos de unos pocos.

La información de las personas, en la actualidad, se ha vuelto imprescindible para realizar cualquier actividad e iniciativa pública y privada; por ende, resulta importante proteger esta información para que no existan abusos ni vulneración de derechos (Sánchez 1998, 26). Para entender la importancia de la protección de los datos personales en la TIDP, se debe partir de la noción de dato.

El dato

Cualquier discusión sobre la protección de datos debe tener claridad sobre el significado de los términos «información» y «dato», que, aunque puedan parecer sinónimos, no lo son. Autores como González (2015, 36) indican que la «información» es un conjunto de datos estructurados en función de determinados fines, mientras que «el dato», por sí solo, es una referencia y no resuelve una consulta determinada. Para Davara (2011, 37), el dato pasa a ser relevante y objeto de protección legal cuando se une a una persona, ya que ahí se convierte en información personal. Al respecto, la Corte Constitucional ecuatoriana, en la sentencia No. 001-14-PO-CC, señala que: «[...] el dato adquiere la calidad de información en tanto cumple una función en el proceso comunicativo».

No obstante, la diferenciación que delimitan estos autores y la Corte Constitucional ecuatoriana no se orienta al soporte, tipo de manifestación, diversidad de la fuente o pauta de expresión, sino a su funcionalidad. Para Naranjo (2017, 73), esta «[...] debe ser adecuadamente contextualizada, ya que no puede significar que el derecho a la protección de datos se vea limitado o restringido a proteger únicamente información personal [...]», ya que los datos personales no requieren carga informativa para ser objeto de protección. Por ejemplo, en la UE, el GDPR utiliza el término «dato» porque lo considera un concepto lo suficientemente amplio como para abarcar todo tipo de información. Lo que Uicich (1999, 40) reafirma al indicar que un dato, aunque parezca irrelevante o inocuo por el avance tecnológico, quienes tengan acceso a ese dato están en la capacidad de formar el perfil de una persona. Así pues, por la importancia y el cuidado que requieren los datos personales surge la necesidad de regular su tratamiento.

Datos personales

Los datos personales pueden ser tan sencillos como los nombres y apellidos, tan complejos como los datos biométricos, o tan sensibles como aquellos 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 «Me gusta» en Facebook. En realidad, hay miles de formas en las que nuestra propia cotidianeidad nos hace identificables (Gil 2016, 45).

El dato personal[1] puede ser entendido como un tipo de información que permite identificar concretamente a una persona. De manera más específica, las Directrices sobre Protección de la Privacidad y Flujo Transfronterizo de Datos Personales, de la Organización para la Cooperación y el Desarrollo Económico (OCDE), actualizadas en 2013, lo definen como «toda información relativa a un individuo identificado o identificable» (OCDE, 2013). Similares conceptos se encuentran en el derecho comparado, por ejemplo, en el artículo 2 de la Ley Argentina de Protección de Datos Personales, donde se conceptualiza a ellos como la «[...] información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables [...]».

En esta línea, 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». El Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE, en su Dictamen número 4/2007, y el GDPR en su artículo 4, punto 1, acoge en su definición de dato personal. De estas se puede destacar los siguientes elementos: cualquier información sobre persona física e identificada o identificable.

1 Para efectos de la presente investigación, las palabras dato e información se entienden como sinónimos solo en este caso.

El elemento «toda información» o «cualquier información» se puede considerar bastante amplio. Para autores como Zaballos (2013, 140), esto se debe a que los legisladores no tratan de proteger un tipo de dato personal en concreto, sino pretenden evitar los efectos que podría tener el tratamiento de un conjunto de datos personales, muchos intrascendentes, pero susceptibles de entregar información relevante en función del TDP que se realice. Se busca «[...] que no quede por fuera del ámbito de protección ningún tipo de dato ni de soporte sea este físico o virtual» (Naranjo 2017, 68). Por lo cual, realizan una descripción amplia, de modo que se pueda acoger todo tipo de datos personales.

Según el artículo 9 del GDPR, los datos personales sensibles pueden revelar aspectos como el origen racial o étnico, las opiniones políticas o las convicciones religiosas o filosóficas; así como los datos relativos a la salud o la sexualidad. En ese sentido, ya que pueden afectar la esfera íntima de su titular, y originar una discriminación ilícita o arbitraria, las legislaciones extranjeras (como la argentina y la europea) le otorgan un ámbito de protección especial.

El elemento «sobre» remarca que la información debe ser concerniente y relacionarse directamente con una persona física. Por lo tanto, se excluye la protección de datos personales relativos a personas jurídicas, aunque en el derecho comparado podemos encontrar el reconocimiento de datos personales a personas jurídicas, como en la Ley de Protección de Datos Personales uruguaya.

Por último, para que una persona sea identificada, la información disponible de ella debe indicar a quién le pertenece sin la necesidad de realizar una investigación posterior (Gil 2016, 47). En cambio, una persona física es identificable, según el GDPR, cuando su identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Ya que, en varias ocasiones, los datos personales son utilizados para fines ilícitos, sus titulares deben contar con los medios adecuados para proteger su información.

Protección de datos personales

La protección de datos personales surge en la década de los 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 la base 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, cuyo desarrollo se origina en la doctrina del Privacy Law, propuesta 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 establecer en qué medida se puede comunicar a otros sus datos personales (es una idea creada por Alan Westin en 1967, que da inicio al desarrollo de la materia en Europa (Lucena 2012, 129)). Al respecto, Torres (2010, 9) indica que:

> [...] concepto de protección de datos nació como una mera contraposición a la interferencia en la vida privada de las personas facilitada por el avance tecnológico. Sin embargo, con el transcurso del tiempo, esa concepción fue evolucionando hasta llegar al momento actual en el que la doctrina internacional lo entiende como la protección jurídica de las personas en lo concerniente al tratamiento de sus datos personales.

La protección de datos personales surgió para resguardar el derecho a la privacidad de las personas. Sin embargo, con el tiempo llegó a ser un mecanismo jurídico que otorgó a la persona el control y disposición de todos sus datos (Sanz 2008, 139). Por ello, Enríquez (2017, 4) señala que los objetivos principales de la protección de datos son: establecer qué datos deben ser considerados personales; regular y determinar quiénes son los encargados y responsables del TDP; y establecer un nivel adecuado de protección para la TIDP.

La protección de datos personales, a más de ser un medio para el desarrollo económico de los países, es una herramienta necesaria para

garantizar otros derechos. En Ecuador, a partir de la Constitución del año 2008, se establece a la protección de datos como un derecho de libertad de todos los ciudadanos, lo cual, de manera similar, sucede en otros países de Latinoamérica. A continuación explicaremos concretamente qué abarca la protección de datos personales y en qué se fundamenta.

Fundamento

Para comprender lo que engloba la protección de datos y su fundamento, se debe señalar al derecho a la intimidad como su fuente primigenia. Sin embargo, posteriormente se separó progresivamente de ella «[...] hasta que se reconoce su autonomía a través de la jurisprudencia y posteriormente de la incorporación de normativa constitucional, legal e incluso reglamentaria» (Naranjo 2017, 65). Su concepto ha variado según el contexto en el que fuera desarrollado. En Estados Unidos, en su primera aproximación, se lo concebía como correlativo al Right to Privacy, mientras que en Europa se lo entendió como un derecho autónomo frente al derecho a la intimidad y privacidad.

Para Frosini (1983, 101-110), el derecho a la intimidad es un conjunto de facultades que permiten la exclusión de injerencias de terceros en la esfera íntima de la persona. Según Delpiazzo (2007, 11), la protección de datos personales transitó desde un sentido negativo hacia un sentido positivo. De esta manera, no se establecen obstáculos para preservar la integridad de la dimensión interior del individuo, sino que se permite el ejercicio de otros derechos con proyección social e, incluso, económica. Aunque algunos datos personales parezcan insustanciales, estos pueden permitir la formación de perfiles y, por ende, producir consecuencias negativas por valoraciones no deseadas, no autorizadas, equivocadas o inexactas.

Esta postura se enmarca en el razonamiento del Tribunal Constitucional Español, en la sentencia 292/2000, donde se indicó que la protección de datos personales tiene una naturaleza autónoma, pues se concibe como una garantía del titular de los datos personales disponer de estos

datos, cualquiera sea su naturaleza, y no solo los que forman parte de su intimidad. Es decir, el objeto de la protección de datos no se reduce a los datos íntimos de la persona; es mucho más amplio, e incluso alcanza a los datos personales públicos. Consecuentemente, esto constituye una protección de la persona y de sus datos personales ante la manipulación o injerencia no autorizada por la ley.

Derecho fundamental

La protección de los derechos fundamentales ha variado con el paso del tiempo. No siempre se ha concedido el mismo nivel de protección ni se ha reconocido los mismos derechos fundamentales. Estos surgen para solucionar las necesidades cambiantes de la sociedad. Por ejemplo, el derecho a la protección de datos personales se desarrolló por la evolución de la tecnología que, aunque ha aportado significativamente al desarrollo de la sociedad, trajo consigo diversas amenazas y riesgos. La Corte Constitucional de Colombia, en la sentencia C-748/11, explica que el derecho a la protección de datos personales, el cual emergió como una garantía a la vida privada, luego pasó a ser entendido como el derecho a la autodeterminación informativa y, finalmente, como un derecho autónomo. Criterio que la Corte Constitucional ecuatoriana, en la sentencia No. 2064-14-EP/21[2], recoge y desarrolla al aceptar una acción de *habeas data*.

El desarrollo de este derecho se ha realizado fundamentalmente en Europa, como lo demuestran los diversos instrumentos jurídicos que regulan este tema. Por ejemplo, la Carta Europea de Derechos Fundamentales lo reconoce de forma autónoma. Por esta razón, para entender el carácter de este derecho, es necesario partir de una definición de derecho fundamental. Para Ferrajoli (2007, 291) son los:

2 Esta sentencia constituye un precedente constitucional importante en virtud de que amplió el concepto de dato personal como objeto de protección del *hâbeas data;* y, adicionalmente, estableció que el acceso y difusión de imágenes personales de carácter altamente sensible sin el consentimiento expreso de su titular es una vulneración del derecho a la protección de datos personales y autodeterminación informativa, a la imagen, a la honra y buen nombre e intimidad.

> [...] derechos subjetivos que corresponden universalmente a todos los seres humanos en cuanto dotados de estatus de personas, de ciudadanos o personas con capacidad de obrar; entendiendo así por derecho subjetivo, cualquier expectativa positiva (de prestación) o negativa (de no sufrir lesiones) adscrita a un sujeto por una norma jurídica.

Calificar a un derecho como fundamental implica ofrecer a su titular una serie de mecanismos de protección, para garantizar el bien jurídico tutelado. Un derecho fundamental es un todo, un conjunto de propiedades formales y materiales (Pulido 2015, 1571-1575). Así pues, 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 ficheros públicos o privados, o saber el contenido, uso y destino de la información contenida en estos ficheros (Guzmán 2013, 114). Asimismo, este derecho tiene un carácter instrumental frente a otros derechos reconocidos, pues, por un lado, permite a la persona el mantenimiento y desarrollo de su individualidad, la protección de sus derechos, bienes personales, sociales, familiares y patrimoniales; y por otro, porque el uso indebido de datos personales puede afectar otros derechos, como el de educación o salud (Puccinelli 1999, 68).

El derecho a la protección de datos personales otorga facultades positivas de disposición y control de sus datos, a diferencia del derecho a la privacidad, el cual confiere facultades negativas de exclusión a terceros de la vida privada de una persona (Remolina 2015, 89). En palabras del Tribunal Constitucional Español, en la sentencia 292/2000, es «[...] un poder de disposición y de control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero. Además, de saber quién y para qué los posee».

Por otro lado, a pesar de su alcance, el derecho a la protección de datos personales no se concibe como ilimitado. Existen diferentes razones por las que se establecen límites, por ejemplo, para una TIDP «[e]l 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» (Garriga 2016, 94). Los datos son necesarios para realizar varias actividades lícitas, legítimas y de interés general o particular. Por eso, el derecho a la protec-

ción de datos no implica oponerse al tratamiento de datos, sino solicita exigir uno correcto (Remolina, Tenorio y Quintero 2018, 48).

En síntesis, la protección de datos personales es un derecho autónomo, pues protege todo tipo de datos de carácter personal, y no solo los relativos al ámbito más íntimo de la vida privada. Es un derecho de carácter instrumental, ya que a través de él se garantiza a las personas el pleno ejercicio de todos sus derechos fundamentales, como el acceso a la educación, vivienda, crédito, entre otros (Villalba 2017, 38). Su contenido conlleva una pluralidad de derechos básicos, principios y garantías que lo convierte en un derecho complejo (Valverde 2013, 21). De tal forma, para que su ejercicio sea efectivo, por medio de él se debe 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, la limitación del tratamiento y el derecho al olvido. Todos ellos, en conjunto, se denominan derechos AROLPOD.

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 dominio sobre esos datos. Con el fin de preservar este derecho fundamental, se necesita aplicar una serie de principios y criterios específicos para su tratamiento (Sanz 2008, 139). De acuerdo con Alexy (1993, 458), los principios son mandatos de optimización, normas que ordenan la realización de algo según las posibilidades jurídicas y reales. Diferentes instrumentos jurídicos internacionales han establecido una serie de principios que velan por el respeto a la protección de datos personales. Sin embargo, en el GDPR se puede encontrar los más importantes y lo que la mayoría de las legislaciones sobre protección de datos ha tomado como modelo. A continuación, de manera sistematizada, se desarrollarán estos principios.

Tabla 1. Principios rectores de la protección de datos personales

Principio	Explicación	Instrumentos jurídicos
Licitud	Exige a los responsables del TDP observar las reglas que están definidas en la Ley. Los datos personales no pueden obtenerse por medio de métodos engañosos o fraudulentos (Mendoza 2017, 276). El TDP tiene que hacerse siempre con apego a la normativa aplicable y conforme a lo acordado entre el responsable del tratamiento y el titular de los datos personales, a través de los medios permitidos por la norma.	RIPD (2017), GDPR (2016), OCDE (2013), APEC (2004), Ley de protección de datos de: Argentina (2000), México (2017), Brasil (2018).
Lealtad	Implica tratar los datos sin engaño y de la forma como se ha indicado, según el considerando 39 y 60 del GDPR. Para los titulares de los datos debe quedar totalmente claro qué se hace con sus datos. En un TDP «[...] debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal» (Guashc 2012, 425).	RIPD (2017), GDPR (2016), OCDE (2013). Ley de protección de datos de: Argentina (2000), México (2017), Brasil (2018).
Transparencia	Supone facilitar al ciudadano información sobre el tratamiento de sus datos personales, de una manera que resulte accesible y fácil de entender. El titular de los datos debe obtener, en cualquier momento y sin restricciones, información acerca de la existencia, cómo se trata y cualquier otra información sobre los datos que le conciernan (Monsalve 2016, 176).	RIPD (2017), GDPR (2016), OCDE (2013), APEC (2004), Ley de protección de datos de: Argentina (2000), México (2017), Brasil (2018).
Finalidad	Se fundamenta en que el TDP se realizará únicamente en el ámbito de finalidades legítimas, explicitas y determinadas. Sus fines deberán estar precisamente determinados (Ortiz 2002, 134). Se busca que el tratamiento tenga como objetivo la realización de actividades concretas, legítimas y conocidas por el titular del dato. No pueden ser tratados para fines incompatibles o distintos a los que motivaron su recogida (Zaballos 2013, 204).	RIPD (2017), GDPR (2016), OCDE (2013), APEC (2004), Ley de protección de datos de: Argentina (2000), México (2017), Brasil (2018).

Proporcionalidad o minimización de datos	Según el art. 5 numeral 1 literal c del GDPR, el responsable del TDP solo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento. Los datos que serán objeto de TDP deben responder al fin para el que fueron recogidos, ya que «[...] no está permitido recolectar o usar datos que no guarden estrecha relación con la finalidad del tratamiento» (Remolina et al. 2018, 60).	RIPD (2017), GDPR (2016), OCDE (2013), APEC (2004), Ley de protección de datos de: Argentina (2000), México (2017), Brasil (2018).
Exactitud	Según este principio, los responsables del TDP «[...] deben tomar las medidas necesarias para que los datos que se encuentren inexactos o incompletos, en determinación con los fines por los cuales fueron recogidos o tratados, sean suprimidos o rectificados» (Alfaro y Arguedas 2015, 35).	RIPD (2017), GDPR (2016), OCDE (2013), APEC (2004), Ley de protección de datos de: Argentina (2000), México (2017), Brasil (2018).
Vigencia	Para garantizar un adecuado TDP «[...] los datos personales no se deben tratar indefinidamente sino solo por el período de tiempo necesario para cumplir la finalidad para la cual fueron recolectados» (Remolina *et al.* 2018, 62). Deben ser mantenidos durante el tiempo necesario para los fines del TDP.	GDPR (2016), OCDE (2013), APEC (2004), Ley de protección de datos de: Argentina (2000), México (2017), Brasil (2018).
Seguridad	Este principio impone al responsable del TDP emplear medidas técnicas, organizativas y salvaguardas razonables de seguridad para proteger los datos personales contra riesgos que presenta el TDP, como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación (Zaballos 2013, 348). Es necesario adoptar y emplear todas las medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole para proteger los datos personales (Remolina *et al.* 2018, 64).	RIPD (2017), GDPR (2016), OCDE (2013), APEC (2004), Ley de protección de datos de: Argentina (2000), Brasil (2018).
Responsabilidad proactiva	Supone una obligación del encargado o responsable del TDP «[...] estar en la capacidad de demostrar que el interesado otorgó su consentimiento para el tratamiento de los datos de carácter personal» (Quesada 2017, 56). Implica, según el GDPR, que los responsables y encargados del tratamiento deben adoptar y utilizar medidas apropiadas, efectivas y verificables que le permitan probar el correcto cumplimiento de las normas sobre protección de datos.	RIPD (2017), GDPR (2016), OCDE (2013), APEC (2004), Ley de protección de datos de: Argentina (2000), Brasil (2018).

Nota: explicación e instrumentos jurídicos internacionales y nacionales que contemplan los principios rectores de la protección de datos.

Tratamiento de datos personales

El TDP se ha convertido en una actividad cotidiana, de alta importancia para el Estado, las empresas y los particulares. Todos requieren de la información personal para tomar y ejecutar decisiones de diversa naturaleza (económica, seguridad nacional, política, laboral, financiera, comercial, entre otros). El TDP rebasa fronteras por la globalización de las actividades, como el comercio electrónico. Por ello, es imperativo contar con una regulación apropiada que permita proteger los derechos de las personas.

La regulación del TDP ha variado a lo largo del tiempo. En un principio fue casi inexistente, pero en la actualidad se han expedido, a nivel mundial, un sinnúmero de normas generales y sectoriales. La regulación del TDP no se opone al uso de datos, sino a su eventual abuso, pues puede provocar una vulneración de los derechos humanos de los titulares de los datos (Remolina *et al.* 2018, 48). Con esta introducción, ahora corresponde señalar qué se debe entender por TDP. Por su importancia, varias organizaciones y países lo definen de distintas maneras. En la siguiente tabla se expondrán las más significativas:

Tabla 2. Definiciones de tratamiento de datos personales

Instrumento Jurídico	Definición
Ley de protección de datos argentina (2000)	Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y, en general, el procesamiento de datos personales, así como su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias (art. 2 literal 4).
Ley de protección de datos en posesión de particulares mexicana (2010)	La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales (art. 3 numeral 18).

Reglamento General de Protección de Datos de la UE (2016)	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 (art. 4 numeral 2).
Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2017)	Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa mas no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y, en general, cualquier uso o disposición de datos personales (art. 2 literal i).

Nota: definiciones de los principales instrumentos jurídicos que definen al TDP.

De las anteriores definiciones, podemos extraer que el TDP puede ser automatizado o no. Conforme el artículo 4 del GDPR, son tres las partes que participan en un TDP: 1) el interesado, que es la persona física cuyos datos personales son objeto de un TDP; 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 es la persona física o jurídica, de naturaleza pública o privada, que trata datos distintos de la persona responsable o lleva a cabo un TDP por cuenta del responsable del TDP.

Con respecto a las fases del TDP, autores como Davara Rodríguez (2006, 69) y Zaballos (2013, 163), de manera similar, señalan que son: la recolección de datos en soportes específicos automatizados o no; el TDP que comprende todas las operaciones que un responsable o encargado del TDP lleva a cabo sobre los datos; y por último, la utilización y comunicación, de ser el caso. Si su uso es interno, no habrá comunicación, pero si su uso es externo sí existirá comunicación, cesión o transferencia, ya que los datos salen del responsable o encargado hacia un tercero. Adicionalmente, una forma con la que se puede dar un TDP es a través de una TIDP. Veámosla a continuación.

Transferencia internacional de datos personales

En 1980, la OCDE señalaba, en sus directrices sobre privacidad, que la TIDP se ha incrementado considerablemente en años recientes y se aumentarán con el desarrollo de las tecnologías y las comunicaciones. 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 y las autoridades de los diferentes países. Estos procesos, junto con el incremento de empresas que participan en los mercados digitales, requirieron expedir normas sobre el TDP, que conciliaran la protección de la privacidad y la TIDP. Es más, la TIDP fue una de las principales razones que motivaron la regulación sobre TDP, siendo parte del «[...] ¿qué? y del ¿por qué? se quería regular y armonizar la protección de datos [...]» (Remolina 2015, 150).

Definición y alcance

Para el GDPR, y para la sentencia Lindqvist contra Gäta hovärtt, del Tribunal de Justicia de la Unión Europea (TJUE), una TIDP se produce cuando los datos personales son enviados fuera del Espacio Económico Europeo a un tercer país u organización internacional, por el responsable o encargado de su tratamiento. De forma más amplia, la TIDP es (Grande 2016, 59) una transmisión, realizada por cualquier medio a través de las fronteras nacionales, de datos personales que sean objeto de un TDP, o cuando se reúnan con el propósito de someterlos a uno.

En Latinoamérica, según el artículo 4 literal h del Decreto No. 414/009, reglamentario para la ley uruguaya de protección de datos personales, la TIDP es una especie de TDP que supone «[...] una transmisión de estos fuera del territorio nacional, constituyendo una cesión o comunicación, y teniendo por objeto la realización de un tratamiento por cuenta del responsable de la base de datos o tratamiento establecido en

territorio uruguayo». Por ende, una TIDP es un proceso de exportación o importación de datos personales, contenidos en una base de datos ubicada en un Estado, que son enviados a otros Estados.

La TIDP se puede dar por varios motivos. Por ejemplo: «[...] 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. De nuevo, un ejemplo de esto sería cuando los datos personales se transfieren desde una compañía ecuatoriana a un prestador de servicios de nube, que se encuentra establecido en Estados Unidos y, a su vez, cuando una empresa que proporciona asistencia técnica a dicho prestador de servicios de nube accede a los datos personales desde la India.

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

Sujetos intervinientes

De las definiciones expuestas, es posible identificar, en la TIDP, la participación de dos partes: el exportador y el receptor de datos. Por la promulgación del GDPR, en relación con la Directiva 95/46/CE, se amplió la definición de receptor de datos. Ahora se incluye también como destinatarios a: las organizaciones internacionales, y uno o varios sectores específicos de un tercer país. Así, en una TIDP tenemos dos personas: 1) el exportador, definido en el artículo 4 literal e, del Decreto No. 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 2) el destinatario, definido por el artículo 4 del GDPR, como: «[...] la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comunican datos personales, se trate o no de un tercero».

En síntesis, una TIDP se puede realizar entre: 1) dos responsables del tratamiento (por ejemplo, uno establecido en España y otro establecido en un tercer país, o si es una organización internacional); 2) un responsable y un encargado del tratamiento, encontrándose el responsable establecido en los Estados Unidos y el encargado del TDP en Francia; 3) dos encargados del TDP, uno asentado en Argentina y otro en Brasil; o 4) a terceros.

Principios propios

Para que los datos personales puedan ser parte de una TIDP, a más de cumplir con los principios rectores de la protección de datos, se debe considerar los principios de continuidad de la protección y el principio de equivalencia, todos ellos necesarios para contar con un nivel adecuado de protección. A continuación se desarrollarán estos principios.

Principio de continuidad de la protección

Un estándar adecuado de protección no puede conllevar una disminución de la protección que previamente obtuvo los datos personales en el país de origen de la persona titular de los datos, cuando estos fueron transferidos internacionalmente. Al respecto, De Frutos, en el VI Encuentro Iberoamericano de Protección de Datos de 2008, indicó que esta regla se conoce como el principio de continuidad de la protección de datos, y «[...] se fundamenta en que la transferencia internacional de datos no debe afectar la protección de los interesados por lo que respecta al tratamiento de sus datos personales». El propósito de este principio es 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 ya contaban en el país de origen. Se busca que el nivel de protección del país exportador se garantice en el país importador.

Principio de equivalencia

A nivel internacional, no todos los Estados ofrecen las mismas garantías en la protección de datos personales. Europa, por ejemplo, cuenta con amplia legislación y jurisprudencia sobre el tema, mientras que países como Venezuela, Bolivia, y no hace mucho Ecuador (mayo 2021), no contaban con una ley de protección de datos. Por esta falta de uniformidad de los ordenamientos jurídicos, se exige, por parte de la mayoría de países que cuentan con una legislación de protección de datos y los instrumentos internacionales (Directrices de la OCDE), para autorizar una TIDP, que el país receptor de datos cuente con un nivel de protección equivalente al que ofrece el país emisor. En términos de Remolina (2010, 497), para una TIDP se debe verificar que el país importador garantice un nivel de protección adecuado de los datos personales.

Exigir un nivel adecuado de protección, para autorizar una TIDP, es un principio de equivalencia, que tiene como finalidad que en una TIDP «[...] el país receptor de datos debe contar con garantías equivalentes a las que ofrece el país transmisor» (Alfaro y Arguedas 2015, 230). En este sentido, según la sentencia del TJUE, de 6 de octubre de 2015, en el caso Schrems, asunto C-362/14, el principio de equivalencia implica que el importador de datos: «[...] garantice 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».

Importancia

Para Remolina (2010, 493), la TIDP que no se encuentre regulada y reglada es un problema, por tres razones principales: 1) disminuye la

protección jurídica de la información y pone al titular de los datos en un estado de vulnerabilidad, al no tener cómo proteger sus datos; 2) constituye una situación desventajosa en el contexto comercial, pues resta competitividad al país porque imposibilita su participación en transacciones comerciales internacionales que involucren TIDP, perjudicando directamente a los empresarios (Garrido 1991, 17); y 3) la protección de datos se relaciona con el concepto de sociedad democrática, por lo que la falta de ella implica una afectación al sistema político que sostiene el Estado de Derecho.

Para Ornelas (2008, 147), un régimen que regule adecuadamente la TIDP debe contar con una regulación equilibrada, que facilite el comercio internacional y, a la vez, proteja los datos personales. De ese modo, los beneficios que obtiene un país al contar con un nivel adecuado de protección para la TIDP son dos: 1) eleva el nivel de protección de la información de sus ciudadanos; y 2) crea un escenario más competitivo para que el país sea un lugar en el que puedan realizarse negocios que implican TIDP.

En el Título VII del Acuerdo que suscribió Ecuador con la UE, se establece una garantía de protección de datos para fomentar el comercio electrónico internacional, cuyo objetivo es reducir las distorsiones y obstáculos entre las partes. La UE es una de las mayores economías mundiales, y una importante fuente que se beneficia de la inversión extranjera. De tal forma, Ecuador, para cumplir con este acuerdo y mejorar sus relaciones con la UE, debe adoptar un estándar adecuado de protección de datos, y así garantizar la seguridad a los titulares de los datos, cuando estos son transferidos.

En síntesis, el derecho a la protección de datos personales busca proteger al titular de los datos, pues un tratamiento inadecuado de los datos de una persona puede impedir el desarrollo de otros derechos, así como perjudicar sus intereses. Por otro lado, el comercio internacional requiere que se transfieran los datos personales para funcionar. Entonces, para lograr un equilibrio entre estos dos intereses, a nivel internacional se ha pretendido armonizar su regulación, de modo que se pueda garantizar, en todos los lugares del mundo, un nivel adecuado de protección de da-

tos personales cuando se realiza una TIDP. Los siguientes capítulos del libro profundizarán sobre la regulación de la TIDP a nivel mundial, y analizarán de qué forma Ecuador debe adecuarse a estas normas para contar con un nivel adecuado de protección para la TIDP.

Capítulo segundo

Estándares para la transferencia internacional de datos personales

La globalización ha ampliado el alcance de los mercados nacionales, lo cual produce un aumento acelerado de la TIDP. Para evitar restricciones a la libre circulación de datos personales, y para no detener el desarrollo del comercio internacional y electrónico, es necesario que los Estados posean un nivel adecuado de protección para la TIDP (Ordoñez 2017, 84). A nivel internacional, la protección de datos personales se maneja principalmente por dos modelos: el europeo y el norteamericano. El modelo europeo se establece en una norma constitucional fundamental, una ley general y una fuerte autoridad de control. En cambio, el modelo norteamericano se caracteriza por ser, prácticamente, un sistema de autorregulación, con un marco jurídico flexible, que reclama poca intervención estatal, pues está enfocado más en normas sectoriales.

En este segundo capítulo, al tener estos modelos una fuerte incidencia en la regulación internacional para la TIDP, los analizaremos para determinar el estándar de protección de datos personales con el que se manejan. Adicionalmente, estudiaremos cómo en América Latina se está regulando la TIDP, tomando como referencia a Argentina, México y Brasil. Por último, analizaremos las regulaciones para la TIDP que han emitido los organismos internacionales, como la OCDE y el Foro de Cooperación Económica Asia-Pacífico (APEC).

Estados Unidos de América

En Estados Unidos, 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 con una reinterpretación de los precedentes en la materia. Hasta entonces, se entendía que el derecho anglosajón solamente «[...] protegía personas físicas o bienes materiales a través del derecho de propiedad, de tal modo que la intimidad relativa a la persona recibía una tutela solo indirecta y a menudo incompleta» (Saltor 2013, 275). Con esta nueva comprensión, se comenzó a tutelar jurídicamente bienes inmateriales, como las emociones, los pensamientos y las sensaciones de una persona física.

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 EUA, en el siglo XX, se dictaron tres leyes que configuran los principios rectores del derecho a la privacidad: 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, de 2000; y el Privacy Shield, de 2016, para regular la TIDP con Europa; la California Consumer Privacy Act (CCPA), de 2018, que entró en vigor en 2020; y la Stop Hacks and Improve Electronic Data Security Act (SHIELD). A continuación, examinaremos las leyes mencionadas.

Del Fredoom of Information Act al Right to Financial Privacy Act

Si bien la Privacy Act (1974) fue una de las primeras protecciones para evitar un uso inadecuado de los datos personales por parte del

gobierno, la FOIA es la que estableció el derecho al acceso de los datos almacenados por los organismos públicos. Conforme esta Ley, la administración pública debe, obligatoriamente, tener listados actualizados que permitan conocer el tipo de información contenida en cada registro de cada organismo del Estado. Con la FOIA, las personas tienen el derecho de solicitar, en instancias judiciales, el acceso a su información, que está almacenada en los registros de las agencias federales.

La Privacy Act regula la recopilación, mantenimiento, uso y difusión de la información personal que figura en bancos de datos del gobierno federal (Sánchez González 2015, 174). Ella se constituyó como una de las primeras y más importantes regulaciones del uso de los datos personales por parte del gobierno, pero su alcance es limitado. Solo puede aplicarse al procesamiento de datos por parte del gobierno federal, y no a los gobiernos estatales ni al sector privado (Levin y Nicholson 2005, 362).

La Privacy Act, en su subsección b, prohíbe la divulgación de información de un sistema de registros sin el consentimiento previo (por escrito de su titular), para la cesión de los datos de la persona. Pero existen doce excepciones legales, entre las que destacan: la divulgación de información para fines estadísticos, por la oficina del Censo y la Oficina de Estadísticas Laborales, y la transmisión de datos a otra agencia del gobierno, dentro del concepto de uso rutinario o para investigaciones del Congreso (Gregorio 2005, 307).

En 1978 se promulgó la RFPA, la cual fue diseñada para proteger la confidencialidad de los registros financieros personales, pero solo del gobierno (Levin y Nicholson 2005, 364). Esta ley entrega confidencialidad a las personas por medio de la restricción del acceso del gobierno a su información financiera; sin embargo, no se toma en cuenta el método utilizado para su registro. En síntesis, los principales aspectos y ámbitos de regulación de estas leyes son:

Tabla 3. Protección de datos en Estados Unidos

Instrumento Jurídico	Ámbito de Regulación	Aspectos Relevantes
Fredoom of Information Act (1966)	Ámbito de regulación público. Señala el proceso por el cual todo individuo puede solicitar acceso a registros o información de las agencias federales.	Establece nueve excepciones y tres exclusiones para que un individuo acceda a registros o información de las agencias federales, por ejemplo: archivos personales, médicos o similares, cuya divulgación constituyera invasión injustificada a la privacidad personal.
Privacy Act (1974)	Ámbito de regulación público. Establece un código de prácticas justas de información que rige la recopilación, mantenimiento, uso y difusión de información personal, que se conservan en un sistema de registros bajo el control de una agencia federal.	Otorga los derechos de acceso, rectificación, y el derecho a demandar por violaciones a la ley. Prohíbe la divulgación de información sin el consentimiento previo por escrito de su titular, pero establece doce excepciones. No aplica a registros en poder del Congreso, los tribunales o gobiernos estatales y locales.
Right to Financial Privacy Act (1978)	Ámbito de regulación público. Proteger la información de los clientes de los bancos e instituciones financieras de una intromisión del gobierno.	Los clientes tienen el derecho a acceder a un registro de todas las divulgaciones hechas de su información personal.

Adaptado de Sánchez González (2015, 174-175) y Levin y Nicholson (2005, 362-365).
Nota: principales aspectos regulatorios de estas leyes.

Por consiguiente, la FOIA, la Privacy Act y la RFPA supusieron grandes desarrollos del derecho a la privacidad en Estados Unidos. Mas, al solamente tener un ámbito de regulación público, no llegaron a constituirse de la forma en la que se lo habían planeado. En cuanto a la TIDP, en ella no se regula estas leyes.

Del Safe Harbour al Privacy Shield

En el artículo 25 de Directiva 95/46/CE, del Parlamento Europeo y del Consejo, se señalaba que la TIDP a terceros países se realiza solamente cuando este garantiza un nivel de protección adecuado. En el apartado 6 se establecía que la Comisión Europea (CE) podrá remarcar que ese país garantiza un nivel de protección adecuado a la vista de su legislación interna o de sus compromisos internacionales. Por la importancia de Estados Unidos, a nivel económico y tecnológico en el mundo, y ya que maneja, junto con Europa, sistemas regulatorios antagónicos, era necesario propiciar un acuerdo que permita instaurar un régimen de protección de datos personales, cuando estos sean transferidos hacia Estados Unidos (Sánchez González 2015, 180).

Mediante la decisión de la CE, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, la CE condicionó el nivel adecuado de protección de la TIDP, que se efectúa desde la UE a Estados Unidos, cumpliendo con los Principios de Puerto Seguro (anexo I) de la decisión. Estos se aplicaban de conformidad con la orientación que proporcionan las preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, el 21 de julio de 2000, y que figuraban en el anexo II de la decisión (Santos 2013, 7).

El Safe Harbour fue un conjunto de principios, negociados entre Estados Unidos y la UE, creados para poder transferir datos personales entre estos territorios. Se constituyó como una institución jurídica que permitía esta actividad 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 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 los organismos

jurídicos competentes en EUA, pero siempre con arreglo a las competencias que sus propias leyes les otorgan. De esta manera, el sistema de protección de datos en EUA es sectorial, y no todos los organismos ni materias están incluidas en este acuerdo. Debido a estos problemas, y a pesar de que miles de empresas norteamericanas se adhirieron al acuerdo, en 2015 la sentencia del TJUE, emitida en el caso Schrems, invalidó la decisión de la CE del 2000, con la que se aprobaba el acuerdo de Safe Harbour, el principal marco jurídico que facultaba a las empresas y organizaciones de la UE el 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 Facebook desde 2008, presentó una reclamación ante el Data Protection Commissioner el 25 de junio de 2013. En ella solicitaba que se prohibiera a Facebook Ireland el transferir sus datos personales a Estados Unidos, pues este país no garantizaba una suficiente protección de los datos personales conservados en su territorio. Schrems, además, hizo referencia a las revelaciones que Edward Snowden hizo en 2013 sobre las actividades de los servicios de información de EUA, particularmente de la National Security Agency.

Según los fragmentos (del 70 al 89) de la sentencia, la invalidez de este acuerdo se dio por la falta de fiabilidad de este marco jurídico, en virtud de cinco razones: 1) los principios del Safe Harbour no son de aplicación obligatoria; 2) la decisión no demuestra que Estados Unidos, como tercer país, garantice un nivel adecuado de protección conforme a la Directiva 95/46/CE; 3) la legislación americana se encontraba por encima de los principios del Safe Harbour; 4) la normativa americana no protege los derechos fundamentales de las personas, cuyos datos se transfieran desde la UE a Estados Unidos; y 5) los procedimientos legales para exigir el cumplimiento de los principios son limitados.

Después de la publicación de la sentencia del caso Schrems, mediante la Declaración del Grupo de Trabajo del artículo 29, el 16 de octubre de 2015, hubo un llamado a toda la comunidad europea a buscar soluciones jurídicas, políticas y técnicas, que permitieran la TIDP a los Estados

Unidos. En la señalada declaración, se instó a las instituciones europeas y a los Estados el iniciar urgentemente negociaciones con Estados Unidos para conseguir una solución antes del 31 de enero de 2016. Como lo explica Uría (2016, 280), «[...] después del término de ese plazo, el 2 de febrero, la Comisión Europea anunció que había alcanzado un acuerdo con Estados Unidos para establecer un nuevo marco normativo: el EU-US Privacy Shield (escudo de privacidad)».

Mediante la decisión de ejecución (UE) número 2016/1250, de la CE, con fecha 12 de julio de 2016, se acordó el Privacy Shield, el cual permitió, de nuevo, realizar TIDP desde la UE a los Estados Unidos, sin la necesidad de abordar la autorización de la entidad de control (Castellanos 2017, 26). Su contenido comprende 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 complementarios. A continuación, compararemos el Safe Harbour y el Privacy Shield, donde se mostrará sus cuestiones más relevantes.

Tabla 4. Comparación entre el Privacy Shield y el Safe Harbour

	Privacy Shield	Safe Harbour
De aplicación obligatoria	X	X
Definición de la TIDP	X	X
TDP especial para datos personales sensibles	X	X
Derechos ARCO	✓	✓
Desarrollo de las TIDP ulteriores	✓	✓
Exigencia de un nivel adecuado de protección para realizar TIDP	✓	✓
Normas corporativas vinculantes	✓	✓
Garantías adecuadas para la TIDP	X	X
Exigencia de la autoridad de control autónoma	X	X

Códigos de conducta	X	X
Obligaciones a los responsables y encargados del TDP	✓	X
Responsabilidad proactiva y demostrada	X	X
Sanciones administrativas o pecuniarias	✓	✓
Principios para la protección de la TIDP	✓	✓

Nota: todas ellas son diferencias entre el Safe Harbour y el Privacy Shield.

Tanto el Safe Harbour como el Privacy Shield se concibieron como mecanismos para solucionar la ausencia de regulación en Estados Unidos del TDP, y para 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 estuvo más tiempo vigente, aunque fue acogido por miles de empresas americanas, no era de carácter obligatorio, no estaba en igual rango que otras leyes americanas y se encontraba desactualizado. Tal estado dificultaba su aplicación y, por ende, tuvo que ser sustituido.

El Privacy Shield, aunque pretendía cubrir los vacíos de su antecesor, presentó los mismos problemas, de suerte que no podía constituirse en un marco regulatorio obligatorio y no garantizaba que los Estados Unidos pudieran ser considerados 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, el 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. De igual manera, el mismo Tribunal, en esa ocasión, confirmó que las cláusulas contractuales estándar siguen siendo una herramienta válida para la transferencia de datos personales a procesadores establecidos en terceros países.

California Consumer Privacy Act

En cuanto a las últimas leyes promulgadas, primero está la CCPA, una ley de privacidad del consumidor que se aprobó en el Estado de California el 28 de junio de 2018 y entró en vigor el 1 de enero de 2020. Desde su fase como proyecto de ley, ha sido descrita como el GDPR en los Estados Unidos. De hecho, 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.

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

El CCPA otorgó a los residentes de California el derecho a: 1) saber qué datos personales se están recolectando; 2) conocer si sus datos personales se venden o divulgan y a quién; 3) oponerse a la venta de datos personales; 4) acceder a sus datos personales; y 5) igualdad en la prestación del servicio y en el precio, incluso si ejercen sus derechos de privacidad. De este modo, las empresas americanas han tenido que mejorar sus políticas de protección de datos, en beneficio de los consumidores (Bryan Cave Leighton Paisner LLP 2018, 7-13). Ahora que sabemos la relación de esta nueva ley con el GDPR, comparemos estas dos normativas jurídicas.

Tabla 5. Comparación entre el GDPR y la CCPA

	GDPR	CCPA
Derechos individuales	→ Avisos a los sujetos de los datos. → Derecho de acceso a los datos. → Derecho al olvido. → Derecho a reparar errores. → Derecho a oponerse al TDP/ revocar consentimiento.	→ Avisos a los sujetos de los datos. → Derecho a ser olvidado. → Derecho de acceso a los datos. → Derecho a optar por la venta de información. → Derecho a recibir servicios en igualdad de condiciones.
Seguridad	→ Se requiere seguridad de datos apropiada. → Notificación de incumplimiento.	Se requiere seguridad de datos apropiada.
Proveedor de servicio	→ Requisitos contractuales en los acuerdos de proveedores de servicios.	Requisitos contractuales en los acuerdos de proveedores de servicios.
Capacidad para procesar datos	→ Propósito permisible. → Minimización de datos.	Ninguna
TIDP fuera de la UE	Las medidas de adecuación requeridas para cualquier país determinado por tener leyes que no sean paralelas a la UE.	Ninguna
Responsabilidad / gobernabilidad	→ Documentación interna y mantenimiento de registros. → Designar un Delegado de Protección de Datos (si es necesario) u otra persona responsable.	Ninguna

Adaptado de Bryan Cave Leighton Paisner LLP 2018, 2.
Nota: todas ellas son diferencias entre el GDPR y el CCPA.

En resumen, la protección de datos, en EUA, sigue orientándose a través de los años por un modelo de autorregulación, que no es eficiente y no garantiza la seguridad a los titulares de datos personales. En cuanto a la TIDP, por su importancia como Estado, países como los de la UE han tratado de buscar algún mecanismo para precautelar los derechos de sus ciudadanos, cuando se tenga que realizar TIDP con Estados Unidos. De ahí nacieron el Safe Harbour y el Privacy Shield, que esencialmente

son normas corporativas vinculantes. Pero, de igual forma, estos marcos jurídicos ni ofrecen ni cumplen con los debidos estándares de protección, como para garantizar adecuadamente el derecho a la protección de datos personales. La CCPA sigue la tendencia del GDPR y muestra que lo decidido en el Estado de California orientará, probablemente, a los demás Estados.

Unión Europea

La regulación sobre protección de datos personales, a menudo, escapa de la esfera de los Estados y transciende al nivel internacional. Europa, después de la Segunda Guerra Mundial, sintió la necesidad y obligación de defender los derechos humanos. Con la cooperación entre sus países, se creó la primera organización internacional en el continente, el Consejo de Europa (CE), gracias al Tratado de Londres del 5 de mayo de 1949 (Cerda 2011, 347). Con el fin de proteger los derechos humanos y promover el Estado de Derecho, el CE adoptó el Convenio Europeo de Derechos Humanos (CEDH), el 4 de noviembre de 1950, que entró en vigor en 1953, teniendo todos los Estados miembros incorporado dicho convenio a su legislación nacional. El derecho a la protección de datos personales encaja en el artículo 8 del CEDH.

Posteriormente, al reflexionar sobre los riesgos que el desarrollo de la tecnología podría implicar para los derechos fundamentales, desde los años setenta los Estados comenzaron a emitir normativas sobre la protección de datos personales, y así reglamentar el TDP. En 1968, el CE expidió la Resolución 509 sobre los derechos humanos y los nuevos logros científicos y técnicos que, si bien no menciona a la protección de datos, directamente tuvo el objetivo de proteger la privacidad ante las nuevas tecnologías (De la Serna 2011, 60). Pero en 1981, el CE adoptó uno de los más importantes instrumentos jurídicos en esta materia: el «Convenio 108» para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

El Convenio 108 puede ser entendido como la primera norma europea que marcó las pautas del modelo común de protección de datos personales, que aún maneja Europa hasta la actualidad (Remolina 2010, 498). Pero para llegar a ese punto, en Europa hubo un desarrollo legislativo y jurisprudencial, tanto a nivel de cada Estado como a nivel comunitario. Por ende, a continuación, haremos un recuento de los instrumentos jurídicos más importantes sobre la protección de datos personales en la UE (desde el Convenio 108 hasta el GDPR), con el fin de entender e identificar los elementos del modelo de protección de datos personales con el que se ha ido manejando la UE.

Antecedentes normativos

La regulación sobre protección de datos personales, en la UE, se ha desarrollado a lo largo del tiempo con gran interés. Por la evolución de las tecnologías de la información y comunicación (TICs), se ha podido realizar un intercambio inmediato de información sin límites físicos. Aquí 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 de 1981, se han emitido varias normas comunitarias que regulan la protección de datos personales. En la siguiente tabla se mostrará el panorama normativo de la UE sobre esta materia.

Tabla 6. Antecedentes normativos en la Unión Europea

Instrumento Jurídico	Ámbito de regulación	Año de expedición
Convenio 108 del Consejo de Europa	Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.	1981
Directiva 95/46/CE del Parlamento y Consejo Europeo	Protección de las personas físicas en lo que respecta al TDP y a la libre circulación de estos datos.	1995
Directiva 97/56/CE del Parlamento y Consejo Europeo	TDP y protección de la intimidad en el sector de las telecomunicaciones.	1997
Directiva 2002/58/CE del Parlamento y Consejo Europeo	TDP y protección de la intimidad en el sector de las comunicaciones electrónicas (directiva sobre la privacidad y las comunicaciones electrónicas)	2002
Directiva 2006/24/CE del Parlamento y Consejo Europeo	Modifica la Directiva 2002/58/CE, relacionada con la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.	2006
Directiva 2009/136/CE del Parlamento y Consejo Europeo	Modifica la Directiva 2002/22/CE, relativa a los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al TDP y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) N° 2006/2004 sobre la cooperación en materia de protección de los consumidores.	2009
Reglamento (EU) 2016/679 (GDPR) del Parlamento y Consejo Europeo	Derogación de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al TDP y a la libre circulación de estos datos.	2016

Adaptado de Rojas 2014, 112.
Nota: todas ellas remarcan el desarrollo normativo en la UE sobre protección de datos personales.

Junto a la normativa comunitaria, los Estados que conforman la UE, en su legislación interna, fueron emitiendo 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. Pero una de las

más significativas es la Ley Federal de Protección de Datos, de Austria, que en 1978 consagró, en el artículo 1, el derecho fundamental de todo ciudadano a la confidencialidad del tratamiento y comunicación de sus datos personales.

Al mismo tiempo que la regulación normativa sobre protección de datos personales, en la UE hubo un importante desarrollo jurisprudencial: 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 el derecho a la protección de datos personales como un derecho autónomo e independiente del derecho a la vida privada, e instituyó el primer paso para la construcción y desarrollo del derecho.

Para hacer aquello, el Tribunal alemán partió de la autodeterminación del individuo, argumentando que esta presupone, en las condiciones actuales de tratamiento de información, la libertad de la persona de decidir cómo debe ser tratada su información. En términos del tribunal alemán, en la sentencia 209/83:

> «[…] la libre eclosión de la personalidad presupone en las condiciones de la elaboración moderna de datos, la protección del individuo contra la recogida, almacenamiento, utilización y difusión ilimitadas de sus datos personales queda englobada en el derecho general de protección de la persona del artículo 2º, párrafo 1º, de la Ley Fundamental».

Respecto a la TIDP, para guardar armonía entre las leyes nacionales respecto a la protección de datos, el Convenio 108 requiere una «protección equivalente» entre los países partes, y provee mecanismos de asistencia recíproca y cooperación internacional a través de las autoridades locales de cada país. Las normas de regulación del Convenio 108 fueron la base sobre la que se elaboró la Directiva 95/46/CE, del Parlamento y del Consejo, el 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al TDP y a la libre circulación de estos datos. Posteriormente, se produce el reconocimiento explícito del derecho a la protección de los datos personales en la Carta de los Derechos Fundamentales de la UE, el

7 de diciembre del 2000, el cual ratifica los derechos reconocidos por las tradiciones constitucionales y las obligaciones internacionales comunes de los Estados miembros.

Durante la vigencia de la Directiva 95/46/CE, los Estados miembros de la UE, para cumplir con las obligaciones que les imponían, fueron elevando progresivamente el nivel de protección de los datos personales, produciéndose «[...] 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 2014, 22).

La Directiva 95/46/CE se encontraba estructurada en siete capítulos, los cuales establecían su objeto, definían términos esenciales, delimitaban su ámbito de aplicación, indicaban las condiciones generales para la licitud del TDP, hacían referencia a los principios del derecho a la protección de los datos personales y a los derechos que gozan los titulares de los datos objeto de tratamiento, señalaban los recursos judiciales, responsabilidad y sanciones, regulaban la TIDP, explicaban la elaboración de Códigos de Conducta, trataban sobre la Autoridad de Control y hablaban sobre las medidas de ejecución comunitarias.

Es de nuestro interés el capítulo IV de la Directiva 95/46/CE, pues regulaba la TIDP. Allí se mencionaba dos distintos niveles de protección de datos personales: un nivel de protección equivalente, en el caso de TIDP entre los países miembros de la UE, y un nivel adecuado de protección, en el caso de los flujos de datos hacia terceros países. El carácter adecuado del nivel de protección se evaluaba por la CE mediante una Decisión de Adecuación, considerando diferentes criterios: la naturaleza de los datos, la finalidad y la duración del tratamiento o los tratamientos previstos, el país de origen y el país de destino, el ordenamiento jurídico vigente en el país tercero del que se trate, las normas profesionales y las medidas de seguridad en vigor en dichos países; todo esto conforme al artículo 25 de la Directiva 95/46/CE. Estos criterios aumentaron con la promulgación del GDPR en 2016.

General Data Protection Regulation

En Europa, el 27 de abril de 2016 se adoptó el Reglamento (UE) 2016/679 del Parlamento y del Consejo, con el que se derogó la Directiva 95/46/CE para reformar la normativa ya existente sobre protección de datos personales, y así adaptarla al nuevo contexto mundial, que después del caso 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 las que eran necesarias. Además, siendo de obligatorio cumplimiento y aplicación directa en los Estados pertenecientes a la UE, no requiere transposición, lo cual acelera la eficacia de la aplicación de la norma en los Estados (Ortega y Domenech 2018, 4). Esta novedad pretende transitar 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. Asimismo, para realizar una TIDP se requiere un nivel adecuado de protección, por lo que Estados Unidos debió implementar el Privacy Shield. Latinoamérica se encuentra en proceso de adopción y aplicación de estándares internacionales para la protección de datos personales.

En el GDPR existen tres vías por las que se puede realizar una TIDP, y estas tienen distintos niveles de protección. La vía y el nivel más riguroso es una transferencia basada en una decisión de adecuación. La Comisión Europea, después de una evaluación global del ordenamiento jurídico de un país, declara que cuenta con un nivel adecuado de protección. De tal manera, para analizar exhaustivamente este tema, explicaremos en la siguiente tabla los niveles de protección para la TIDP.

Tabla 7. Niveles de protección para realizar una TIDP

Nivel de protección para la TIDP	Medio por el que se realizará una TIDP	Elementos que debe cumplirse
Nivel adecuado	Decisión de autoridad de control competente (en el caso de la EU la Comisión) de que garantiza un nivel de protección adecuado. La TIDP por este medio no requerirá ninguna autorización específica.	Estado de Derecho. Respeto a los derechos humanos y las libertades fundamentales. Legislación pertinente. Autoridades de control independientes (poderes de ejecución). Normativa internacional vinculante y aplicable.
Garantías adecuadas	Las garantías adecuadas podrán ser aportadas por los siguientes medios: Sin autorización expresa de la autoridad de control: **a)** Instrumento jurídicamente vinculable y exigible entre las autoridades u organismos públicos. **b)** Normas corporativas vinculantes. **c)** Cláusulas tipo de protección de datos. **d)** Código de conducta. **e)** Mecanismo de certificación. Además, los interesados cuentan con derechos exigibles y acciones legales efectivas. Con autorización de autoridad de control: **a)** Cláusulas contractuales. **b)** Acuerdos administrativos.	Estos medios para realizar TIDP deberán, como mínimo, especificar los siguientes elementos: **a)** Información del grupo empresarial. **b)** La finalidad acerca de la TIDP o el conjunto de TIDP que se va a realizar. **c)** Su carácter jurídicamente vinculante (Legalidad). **d)** Aplicación de principios generales en materia de protección de datos. **e)** Derechos a los interesados en relación con el TDP y los medios para ejercerlos. **f)** La aceptación de responsabilidad del responsable o encargado del TDP. **g)** Acceso a los interesados a información sobre las normas corporativas vinculantes. **h)** Funciones de los delegados de protección de datos. **i)** Procedimientos de reclamación. **j)** Mecanismos para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. **k)** Mecanismos para comunicar y registrar las modificaciones a las normas corporativas vinculantes. **l)** Mecanismos de cooperación con la autoridad de control competente. **m)** Mecanismos para informar a la autoridad de control competente de cualquier hecho. **n)** Formación en protección de datos.
Normas corporativas vinculantes	Norma corporativa vinculante aprobada por la autoridad de control competente.	Deben ser jurídicamente vinculantes, aplicarse y ser cumplidas por los responsables y encargados del TDP. Además, deben conferir expresamente derechos a los interesados. Además, las normas corporativas, como mínimo, deben especificar los elementos señalados para la TIDP mediante garantías adecuadas.

Nota: son análisis de los niveles de protección para la TIDP de los arts. 45, 46 y 47 del GDPR.

Adicionalmente, si no es posible cumplir con alguno de estos niveles de protección, una TIDP puede realizarse en los siguientes casos, conforme el artículo 49 del GDPR:

a. Consentimiento explícito del interesado.
b. La TIDP es necesaria para la ejecución de un contrato entre el interesado y el responsable del TDP.
c. La TIDP es necesaria para le ejecución de medidas precontractuales adoptadas a solicitud del interesado.
d. La TIDP es necesaria para la celebración o ejecución de un contrato, en interés del interesado.
e. La TIDP es necesaria por razones importantes de interés público.
f. La TIDP es necesaria para la formulación, el ejercicio o la defensa de reclamaciones.
g. La TIDP es necesaria para proteger los intereses vitales del interesado.
h. La TIDP se realiza desde un Registro Público con arreglo al Derecho de la UE.

También puede realizarse una TIDP en el caso de que esta no sea repetitiva, afecte solo a un número limitado de interesados, sea necesaria para los fines de intereses legítimos imperiosos perseguidos por el responsable del TDP, sobre los que no prevalezcan los intereses, derechos y libertades del titular de los datos.

Como podemos ver, estas tres vías y casos excepcionales son el estándar europeo de protección para realizar una TIDP. Se diferencia bastante del americano, que solo cuenta con normas corporativas vinculantes para la TIDP. Estos criterios se usarán en el siguiente capítulo para determinar el estándar de protección que requiere Ecuador. En la siguiente tabla realizaremos una comparación entre la Directiva 95/46/CE y el GDPR con respecto a la TIDP y a los niveles de protección requeridos en cada una.

Tabla 8. Comparación entre la Directiva 95/46/CE y el GDPR

	Directiva 95/46/CE	GDPR
De aplicación obligatoria	✓	✓
Definición de TIDP	X	X
Desarrollo de las TIDP ulteriores	✓	✓
Principios para la protección de la TIDP	✓	✓
Derechos ARCO	✓	✓
TDP especial para datos personales sensibles	✓	✓
Exigencia de normas sectoriales para la protección de datos	✓	✓
Exigencia de un nivel adecuado de protección para realizar TIDP	✓	✓
Decisión de adecuación para la TIDP	✓	✓
Garantías adecuadas para la TIDP	✓	✓
Normas corporativas vinculantes	X	✓
Casos excepcionales para la TIDP	✓	✓
Exigencia de autoridad de control autónoma	✓	✓
Mecanismos de seguridad	✓	✓
Mecanismos de certificación	X	✓
Códigos de conducta	✓	✓
Delegado de protección de datos personales	X	✓
Obligaciones a los responsables y encargados del TDP	✓	✓
Responsabilidad proactiva y demostrada	X	✓
Sanciones administrativas	✓	✓
Sanciones pecuniarias	✓	✓

Nota: son cambios sustanciales entre la Directiva 95/46/CE y el GDPR respecto a la TIDP.

Regulación de la protección de datos personales en América Latina

En América Latina, la protección de datos personales sigue un ritmo propio y tiene ciertas características que ameritan analizarse. Por ejemplo, recién en el siglo XXI se incorporó, a nivel constitucional, la protección de datos personales como derecho autónomo, por la necesidad de dar respuesta al proceso de evolución tecnológica (Ordóñez 2017, p. 85) y a los peligros de un uso indiscriminado e ilícito de datos, por parte de las plataformas digitales. ¿La razón? 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, con lo que ponen en riesgo la información de las personas (Remolina *et al.* 2018, 68).

Ahora bien, para mostrar cómo se regula la protección de datos en Latinoamérica, se tomará como referencia a tres países (Argentina, México y Brasil). La legislación de cada uno de ellos se comparará con los modelos de protección de datos personales americano y europeo, haciendo énfasis en su desarrollo y en cómo se ha seguido las tendencias regulatorias mundiales sobre este tema en Latinoamérica.

República de Argentina

En el artículo 43 de la Constitución de la República de Argentina se consagra el derecho a la protección de datos personales. Allí se deriva la obligación de los organismos públicos de garantizar el acceso a la información, confidencialidad, supresión y rectificación de los datos personales. Pero es en la Ley 25.336, promulgada el 4 de octubre del 2000, donde se reglamenta la protección de datos personales. En el artículo 2 de la referida Ley se regula la protección de datos personales, sin hacer distinción entre el ámbito público y privado, por lo que es aplicable tanto a entidades privadas como públicas.

En el capítulo 2 de la Ley 25.326 se establece los principios generales en materia de protección de datos personales y TDP. En él se destacan el principio de licitud para la formación de archivos de datos. Por otra parte, el principio de calidad de datos se traduce en que su recolección no puede hacerse por medios desleales, que dichos datos deben ser ciertos y exactos, y su almacenamiento debe permitir el derecho de acceso a su titular. El principio de la información debe comunicar a los titulares para qué serán tratados los datos y quiénes serán sus destinatarios, junto con el principio de responsabilidad demostrada.

En Argentina, conforme el artículo 29, el órgano de control que gozará de autonomía funcional y actuará 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. Esta es la encargada de supervisar el cumplimiento de las disposiciones contenidas en la Ley 25.326, en la Ley de Acceso a la Información y en la Ley del Registro No Llame. Respecto a la TIDP, se sigue el modelo europeo toda vez que en el artículo 12 se exige, para autorizar una TIDP, que el Estado receptor de los datos cuente con un nivel adecuado de protección.

Estados Unidos Mexicanos

El caso mexicano es particular. Con las reformas constitucionales del 2007 y 2009 apenas se empieza a proteger constitucionalmente los datos personales, se consagra explícitamente el derecho a la protección de los mismos y se establecen los derechos ARCO como núcleo fundamental de dicho derecho (Da Cunha 2011, 323). Posteriormente, en 2010, se adopta la Ley Federal de Protección de Datos en Posesión de Particulares, teniendo una aplicación únicamente privada. Dada la redacción de esta Ley, es evidente que se basa en el marco normativo europeo, y 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 mencionada Ley, se establece una serie de principios para la protección de datos personales, como son: el de información, licitud, consentimiento, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. En el 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). También el capítulo IV, según el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, del 21 diciembre de 2011, regula los derechos ARCO. En capítulo V se desarrolla la TIDP, pero no se exige un nivel adecuado de protección, tan solo se requiere el consentimiento del titular de los datos. Asimismo, enumera ciertos supuestos que no requieren consentimiento, además de no desarrollar las transferencias ulteriores.

El 26 de enero de 2017 se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 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». Los particulares, sean personas naturales o jurídicas, no son aplicables en 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 Ley aplicable a sujetos obligados, en relación con la Ley aplicable a privados, se aumenta y desarrolla un grupo 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. Sobre la autoridad de protección de datos personales, ella establece que es el INAI. Por otro lado, respecto a la TIDP, en el artículo 68 de la Ley aplicable a los sujetos obligados indica que:

> [...] el responsable sólo 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.

Gracias a esta norma podemos evidenciar que, para autorizar una TIDP, se reclama el cumplimiento de garantías adecuadas. Además, recalca que se necesita que el responsable del TDP entregue el consentimiento del titular de los datos, y deberá comunicar al receptor de los datos personales las finalidades conforme a 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.

República Federativa del Brasil

Si bien la Constitución brasileña no reconoce explícitamente el derecho a la protección de datos personales, a través de la acción de *habeas data* es posible otorgar protección, conforme el artículo 5 de la Constitución de Brasil. Se concederá *habeas data:* a) para asegurar el conocimiento de la información de una persona que conste en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo. Por esta protección constitucional, Brasil se vio en la necesidad de proteger los datos personales, por lo cual en 2018 promulgó una interesante ley de protección de datos, que entrará en vigor en 2020, la cual regula tanto el ámbito privado como público, siendo muy parecida al GDPR de la UE.

Sobre la TIDP, el artículo 33 de la Ley General de Protección de Datos brasileña (LGPD) indica que solo está permitida en los casos que determina la Ley. Por ejemplo, para países u organismos internacionales que proporcionen un grado de protección de datos personales adecuado, previsto en la LGPD; o cuando el receptor de los datos del país u organización internacional ofrezca y compruebe que entrega garantías de cumplimiento de los principios, derechos

del titular y del régimen de protección de datos, previstos en la LGDP.

La versión del proyecto de ley, presentada tras su aprobación por las cámaras del congreso brasileño, fue vetada en tres aspectos esenciales antes de ser firmada: el establecimiento de una autoridad independiente de protección de datos, las sanciones por la violación de la ley y los requisitos de transparencia para los agentes del sector público que manejan datos personales. No obstante, el 28 de diciembre de 2018, el presidente saliente de Brasil, Michael Temer, firmó la Medida Provisional N° 869/18, con la que se creaba la Autoridad Nacional Brasileña de Protección de Datos. La medida vino a complementar la LGPD y a tratar de remediar los vetos a la LGDP, que dificultarían su adecuada aplicación. La medida creó la autoridad de control, aunque no la dotó de independencia e imparcialidad; elementos necesarios para cumplir con los estándares de protección de datos que se manejan a nivel internacional.

Estándar de protección de datos personales para los Estados Iberoamericanos

La Red Iberoamericana de Protección de Datos (RIPD) surge del Encuentro Iberoamericano de Protección de Datos (EIPD), celebrado en Guatemala, del 1 al 6 de junio de 2003. En él se alcanzó un acuerdo con la asistencia de representantes de 14 países iberoamericanos. Desde 2003, la RIPD se configura como un foro que integra varios actores, tanto del sector público como del privado, para el desarrollo de iniciativas y proyectos relacionados con la protección de datos personales en la región.

Uno de sus documentos más importantes es los Estándares de protección de datos personales para los Estados Iberoamericanos, adoptado en 2017, y aplicable tanto al TDP en el sector privado como en el público. Este acuerdo sigue la línea del Convenio 108, las Directrices sobre

privacidad de la OCDE y el GDPR en cuanto a principios, derechos, sanciones y TIDP con ciertas particularidades, todo lo cual va acorde a las necesidades de los países iberoamericanos. De ese modo, constituyen una serie de directrices para la emisión de normativas regulatorias de protección de datos personales en la región iberoamericana, y sirven, de ser el caso, como referente para la modernización y actualización de las legislaciones existentes.

Tabla 9. Normativa sobre protección de datos personales en América Latina

	Argentina	México	Brasil	RIPD
Norma constitucional sobre la protección de datos	✓	✓	X	-
Legislación general sobre protección de datos personales	✓	✓	✓	-
Derechos ARCO	✓	✓	✓	✓
TDP especial para datos personales sensibles	✓	✓	✓	✓
Medidas de seguridad	✓	✓	✓	✓
Exigencia de autoridad autónoma competente	✓	✓	✓	✓
Recursos administrativos y acciones judiciales	✓	✓	✓	✓
Obligaciones a los responsables y encargados del TDP	✓	✓	✓	✓
Principios para el TDP y la TIDP	✓	✓	✓	✓
Regulación sobre la TIDP	✓	✓	✓	✓
Sanciones	✓	✓	✓	✓

Nota: esta es una comparación entre las normativas de protección de datos de países latinoamericanos y los estándares de la RIPD. El símbolo «-» significa que no aplica.

Organizaciones internacionales que regulan la transferencia internacional de datos

Organización para la Cooperación y el Desarrollo Económicos

El 23 de septiembre de 2018, la OCDE decide adoptar, como una recomendación de su consejo, las directrices sobre política internacional de protección de la privacidad y los flujos transfronterizos de datos personales, fundamentados en los principios que aglutinan a los países miembros de la OCDE: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas. Las directrices sobre la privacidad de la OCDE definen conceptos fundamentales en materia de protección de datos, permiten una aplicación común a los sectores público y privados, y garantizan el libre flujo de datos personales sujetos al respeto de los principios contenidos en las directrices sobre privacidad, como son: licitud, finalidad, proporcionalidad, seguridad, responsabilidad, entre otros. De las directrices de privacidad de la OCDE, surgen, los que más tarde serían, los principios básicos en la protección de datos (Saltor 2013, 107).

Estas directrices exigen un estándar mínimo de protección para el flujo transfronterizo de datos personales; sin embargo, autorizan la restricción del flujo cuando un país no provee un nivel de protección equivalente (Portas 2012, 417). Cabe indicar que, para este nivel equivalente de protección de datos, la presencia de una autoridad de control independiente es necesaria para cumplir con dicho estándar (Cerda 2011, 335). En lo que respecta a la TIDP, el Privacy Framework aumenta el estándar de protección para la TIDP a un nivel adecuado de protección, que garantiza a los titulares el respeto a sus derechos fundamentales cuando sus datos son objeto de una TIDP.

En 2013, la OCDE adopta el documento antes mencionado, mediante el cual se actualizaron las directrices sobre privacidad de 1980. Se

realizaron algunos cambios importantes, por ejemplo: se dejó intactos los principios salvo el de responsabilidad, el cual se desarrolló orientándose a establecer una responsabilidad demostrada, donde el responsable del TDP debe: a) tener un programa de gestión de datos; b) estar en capacidad de demostrar que dicho programa es apropiado para cumplir los principios de la OCDE; y c) notificar a las autoridades y a los titulares de los datos sobre las fallas o brechas de seguridad que afectan los datos personales. Adicionalmente, Remolina (2018, 64) indica que se introdujo el concepto de los programas de gestión de privacidad, que son el mecanismo operativo con el que las organizaciones implantan la protección de privacidad y de los datos personales.

Foro de Cooperación Económica Asia-Pacífico

En 2004 se expidió el Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico (o APEC Privacy Framework). En ese documento se estableció un marco para la regulación del tratamiento de la información personal, adoptado por las economías que integran el APEC. Gracias a él, se procura el establecimiento de un estándar de protección que no detenga el comercio internacional entre los países miembros. Es un programa voluntario, recíproco, multilateral y de cumplimiento de medidas de seguridad, en materia de transferencias transfronterizas de empresas en la región de APEC.

El documento está inspirado en las directivas de 1980 de la OCDE, y tiene como propósito proveer principios generales que guíen la regulación interna de las economías de Asia, en concordancia con la recolección de información personal y las transferencias electrónicas que se realicen entre los países miembros de este organismo. El APEC Privacy Framework, en lo que se refiere a la TIDP, establece que, cuando se realice una TIDP, el controlador de los datos personales debe obtener el consentimiento del individuo o actuar con la debida diligencia y tomar las medidas razonables para asegurar que el receptor de los datos los protegerá consistentemente con los principios de la protección de datos personales, establecidos en su marco regulatorio.

Regulación de la transferencia internacional de datos

Del estudio que hemos realizado, pudimos evidenciar que el derecho a la protección de datos personales se tutela de una manera diferente a nivel mundial; aunque con una tendencia clara para dirigirse al modelo europeo. Además, debido a los riesgos de la TIDP, desde 1980, gracias a las directrices sobre privacidad de la OCDE, se ha marcado una predisposición de los Estados y las organizaciones internacionales para exigir un nivel adecuado de protección de datos personales y autorizar una TIDP. Así pues, a partir del análisis realizado sobre la regulación de la protección de datos personales, corresponde ahora compararlas enfocándonos en los temas que son objeto de la presente investigación, con el fin de delimitar elementos comunes e identificar el estándar adecuado de protección de datos personales para la TIDP aplicable a Ecuador.

Tabla 10. Comparación con respecto a la protección de datos personales

	América Latina			Europa		Organismos Internacionales	
	Argentina	**México**	**Brasil**	**GDPR**	**EEUU**	**OCDE**	**APEC**
Norma constitucional sobre la protección de datos	✓	✓	X	-	X	-	-
Legislación general sobre protección de datos personales	✓	✓	✓	✓	X	✓	✓
TDP especial para datos personales sensibles	✓	✓	✓	✓	X	✓	✓
Exigencia de autoridad autónoma competente	✓	✓	✓	✓	X	✓	✓
Recursos administrativos y acciones judiciales	✓	✓	✓	✓	✓	✓	✓
Obligaciones a los responsables y encargados de los TDP	✓	✓	✓	✓	X	✓	✓

Principios para el TDP y la TIDP	✓	✓	✓	✓	X	✓	✓
Derechos ARCO	✓	✓	✓	✓	X	✓	✓
Sanciones	✓	✓	✓	✓	✓	✓	✓
Regulación sobre la TIDP	✓	✓	✓	✓	✓	✓	✓

Nota: el cuadro es una comparación general entre América Latina, Europa, Estados Unidos y los organismos internacionales, respecto al desarrollo en la protección de datos personales. El signo «-» significa que no aplica.

Tabla 11. Comparación general respecto a la TIDP

	Argentina	México	Brasil	GDPR	EEUU	OCDE	APEC
Definición sobre la TIDP	X	X	✓	X	X	X	X
Desarrollo de las TIDP ulteriores	X	X	✓	✓	✓	✓	X
Exigencia de un nivel adecuado para la TIDP	✓	X	✓	✓	✓	✓	✓
Garantías adecuadas para la TIDP	X	✓	✓	✓	X	✓	✓
Normas corporativas vinculantes para la TIDP	X	✓	✓	✓	✓	✓	✓
Casos excepcionales para la TIDP	✓	✓	✓	✓	✓	✓	✓

Nota: Esta es una comparación de los niveles de protección para realizar una TIDP entre América Latina, Europa, Estados Unidos y los organismos internacionales.

Como se puede notar, Estados Unidos, con el Privacy Shield y la CCPA, al igual que las legislaciones latinoamericanas y los organismos internacionales, se alinean al estándar de protección de datos personales que establece la UE con el GDPR. Se observa 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 al establecer niveles de protección adecuados, que permitan proteger a los titulares de los datos. Además, los parámetros para verificar que un Estado cuente con un nivel de protección aceptable, para autorizar una TIDP, son los que establecía la Directiva 95/46/CE y ahora el GDPR (Bu-Pasha 2017, 219).

En resumen, la regulación de TIDP intenta equiparar dos intereses jurídicos sin que ninguno se vea perjudicado. Por una parte, no impide los flujos transfronterizos de datos personales, necesarios para el comercio internacional y, por otra parte, garantiza que exista una protección de los datos personales cuando estos son transferidos. Por consiguiente, para cumplir con el objetivo de este libro, a continuación se realizará una explicación y estudio de la situación actual de Ecuador respecto a la protección de datos personales y la TIDP.

Capítulo tercero

Estándar adecuado de protección para la transferencia internacional de datos personales en Ecuador

Desde la incorporación y desarrollo de las nuevas tecnologías (Internet), 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 múltiples ventajas: 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, Ecuador, en este contexto, no cuenta con una regulación que garantice un nivel adecuado de protección de datos personales. Esto se evidencia cuando notamos que la protección de datos personales en el país es incompleta, sectorial, contradictoria y desactualizada. De ahí que es insuficiente para proteger adecuadamente los derechos de los titulares de datos personales y, además, inexistente respecto a la TIDP.

Por esta razón, gracias a un recuento y análisis de la normativa que regula la protección de datos en Ecuador, y con las bases obtenidas de los capítulos previos del presente libro, se comprobarán estas aseveraciones. Luego, continuaremos con determinar cuál estándar de protección que debe cumplirse para contar con un nivel adecuado para la TIDP en Ecuador.

Como se evidenció en los capítulos previos, a nivel internacional se requiere cumplir con ciertos parámetros para autorizar una TIDP a un tercer país u organización internacional. Ecuador, por su normativa vigente, no puede responder a estas exigencias. Pero, por los beneficios que pueden traer las TIDP para el país, necesita cumplir con, al menos, estándares de protección mínimos. Esto permitiría el surgimiento de empresas ecuatorianas transnacionales en Internet, con el objetivo de que puedan realizar el TDP de ciudadanos de todo el mundo (Enríquez 2017, 43). De este modo, para determinar cuál estándar internacional de protección para la TIDP, de los que se hemos analizado, puede adaptarse a Ecuador, y, además, para identificar los beneficios que traería contar con una protección adecuada para la TIDP, es fundamental reflexionar sobre las propuestas de ley en la protección de datos personales que se han presentado en el país los últimos años.

Situación actual de la protección de datos personales en Ecuador

En Ecuador se han presentado tres proyectos de ley para regular la protección de datos personales: el primero en 2010, por el asambleísta Vethowen Chica; el segundo en 2016, por la asambleísta Gabriela Rivadeneira; y el tercero en 2019, por la Dirección Nacional de Registros de Datos Públicos (DINARDAP) y el Ministerio de Telecomunicaciones. Este último se convirtió en la primera ley de protección de datos personales de Ecuador. Fue aprobada por la Asamblea Nacional y publicada 26 de mayo de 2021, en el Quinto Suplemento del Registro Oficial 459.

Si bien la ley entró en vigor a partir de su publicación, se suspendió por dos años la aplicación de medidas correctivas o multas, para entregar la oportunidad a los responsables de adaptar su estructura en lo técnico y organizativo. Pero aquello no suspendió el resto de vías legales ante un incumplimiento de la norma, recordando que, en tanto regula el ejercicio de un derecho, las empresas enfrentarían, de manera inmediata, procesos civiles, constitucionales e incluso penales.

Históricamente, Ecuador ha avanzado muy poco en legislación para la protección de datos personales. Solo para la Constitución Política de 1998 se hizo una pequeña referencia al derecho a la intimidad. Sin embargo, desde el siglo XXI se han emitido algunas normativas que tratan de regular la protección de datos personales, y entre ellas se 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 2010. Así, en la siguiente tabla se realizará un recuento del desarrollo normativo de Ecuador sobre esta materia.

Tabla 12. Desarrollo normativo de la protección de datos personales en Ecuador

Cuerpo Normativo	Artículos
Constitución Política de la República del Ecuador (1998)	**Art. 8:** Derecho a la intimidad. **Art. 21:** No discriminación por información personal. **Art. 94:** Hábeas data.
Ley de Seguridad Social (2001)	**Art. 274:** Confidencialidad de los datos personales del asegurado.
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos (2002)	**Art. 9:** Para la recopilación y uso de datos personales se debe garantizar los derechos de privacidad, consentimiento, intimidad y confidencialidad. **Glosario:** definición de dato personal.
Código de la Niñez y Adolescencia (2003)	**Art. 30, núm. 3:** Registros actualizados de datos personales. **Art. 348-C:** Registro en la mediación sin datos personales del adolescente.
Ley Orgánica de Transparencia y Acceso a la Información Pública (2004)	**Art. 6:** Concepto de información confidencial.

Reglamento a la Ley Orgánica de Transparencia y Acceso a la Información Pública (2005)	**Art. 16:** Recurso de Acceso a la información.
Ley Orgánica de la Salud (2006)	**Art. 6, núm. 5:** Confidencialidad de la información sobre enfermedades. **Art. 7, Lit. f:** Confidencialidad en la historia clínica. **Art. 211:** Confidencialidad respecto al genoma individual de la persona.
Constitución de la República del Ecuador (2008)	**Art. 40:** Confidencialidad de los datos personales de las personas ecuatorianas en el exterior. **Art. 66, núm. 19:** Derecho a la protección de datos personales. **Art. 66, núm 20.** Derecho a la intimidad. **Art. 92:** Hábeas data.
Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009)	**Art. 49:** Hábeas data. Derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos.
Ley de Seguridad Pública y del Estado (2009)	**Art. 22:** Prohibición de que un organismo de inteligencia obtenga datos personales sin autorización judicial.
Ley Orgánica del Sistema Nacional de Registro de Datos Públicos (2010)	**Art. 6:** protección especial de datos en personales sensibles.
Código Orgánico Integral Penal (2014)	**Art. 12:** Derecho de protección a los datos personales de las/os persona privada de libertad. **Art. 178:** Delito de violación a la intimidad. **Art. 229:** Delito de revelación ilegal de base de datos.
Código Orgánico Monetario y Financiero Libro I (2014)	**Art. 152:** Derechos de los usuarios financieros. **Art. 235, núm. 18:** Prohibición de comercializar las bases de datos. **Art. 352:** Confidencialidad de los datos de los usuarios del sistema financiero nacional. **Art. 360:** Registro de datos crediticios.
Ley Orgánica de Telecomunicaciones (2015)	**Art. 22, núm. 4:** Derecho de protección de datos personales a los usuarios. **Art. 24, núm. 14:** Obligación de los prestadores de servicios de garantizar la protección de datos personales. **Arts. 78, 79 y 82:** Principios para el TDP.

Código Orgánico General de Procesos (2015)	**Art. 7:** Utilización de los datos personales solamente para la sustanciación de un proceso judicial.
Ley General de los servicios postales (2015)	**Art. 34, núm. 13:** Obligación de los operadores postales de proteger los datos de los usuarios de servicios postales. **Art. 35, núm. 11:** Confidencialidad de los datos de los usuarios de servicios postales.
Reglamento General a Ley Orgánica de Telecomunicaciones (2016)	**Art. 120:** Prohibición de ejecutar u omitir acciones que violen la garantía de protección de los datos personales.
Ley Orgánica de Gestión de la Identidad y Datos Civiles (2016)	**Art. 75:** consentimiento del titular de los datos.
Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos (2016)	**Art. 11:** Principios para el tratamiento de datos públicos. **Art. 12:** Derechos de los titulares de datos públicos.
Reglamento General a la Ley General de los Servicios Postales (2016)	**Art. 7:** Protección de los datos personales de los usuarios de los servicios postales.
Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación (2016)	**Art. 67:** Cumplir en la investigación científica el principio de confidencialidad de los datos personales. **Art. 141:** Utilización de datos personales en contenidos protegidos o no por propiedad intelectual. **Disposición General Vigésima Séptima:** El TDP requerirá autorización previa e informada del titular de los datos.
Ley Orgánica de Movilidad Humana (2017)	**Art. 7:** Derecho de los ecuatorianos en el exterior a la confidencialidad de sus datos. **Art. 94:** Confidencialidad de los datos de las personas en protección internacional. **Art. 99:** Protección de datos personales en el procedimiento de determinación de la condición de refugiado.
Reglamento a la Ley Orgánica de Movilidad Humana (2017)	**Art. 78:** Derecho de un refugiado a la protección y confidencialidad de sus datos.

Reglamento a la Ley Orgánica de Gestión de la Identidad y Datos Civiles (2018)	**Art. 2, núm. 5:** Definición de datos personales. **Art. 93:** Protección especial para datos sensibles.
Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos (2018)	**Art. 5:** Derecho de acceso al titular de los datos. **Art. 6:** Prohibición de cesión o transferencia de datos personales sin consentimiento.

Nota: Es la normativa ecuatoriana que regulaba la protección de datos personales hasta el 26 de mayo de 2021. Un análisis detallado se encuentra en el Anexo 1.

Aunque la Constitución del Ecuador reconoce el derecho a la protección de datos personales, hasta mayo de 2021 no existía una ley de protección de datos, por lo cual se regulaba en varios cuerpos normativos pero de manera incompleta y, en muchos casos, contradictoria.

En estas normas existen algunos parámetros para el TDP de datos públicos, pero no se desarrollaban 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 ejemplo, la limitación al TDP). Además, no se establecía una autoridad de control así como tampoco mencionaban una regulación al TDP, en el ámbito privado, o a la TIDP.

La normativa estaba desactualizada y, en muchos casos, era errónea, ya que los conceptos estaban mal desarrollados y no respondían a los avances tecnológicos, como los conceptos de ficheros o de dato personal. Estas leyes no permitían ejercer el derecho a la protección de datos personales; por esta razón, con el fin de reafirmar que la protección de datos en Ecuador es insuficiente, en la siguiente tabla se realizará una comparación de nuestro país con otros países de la región, sobre los elementos fundamentales que debe ofrecer un sistema de protección de datos personales para proteger los derechos de sus ciudadanos.

Tabla 13. Protección de datos personales en Latinomérica

	Ecuador	Argentina	México	Brasil
Norma constitucional sobre protección de datos personales	✓	✓	✓	X
Legislación general sobre protección de datos personales	X	✓	✓	✓
Principios para el TDP	X	✓	✓	✓
Derechos ARCO	✓	✓	✓	✓
Autoridad de control autónoma	X	✓	✓	X
Recursos administrativos y acciones judiciales	X	✓	✓	✓
Obligaciones a los responsables y encargados de los TDP	X	✓	✓	✓
TDP especial para datos personales sensibles	X	✓	✓	✓
Medidas de seguridad	X	✓	✓	✓
Mecanismos de certificación	X	X	X	✓
Sanciones administrativas	X	✓	✓	✓
Sanciones pecuniarias	X	✓	✓	✓
Regulación sobre la TIDP	X	✓	✓	✓

*Por el *Hábeas Data* se ejercen los derechos ARCO, pero tal como está concebido en la normativa ecuatoriana no permite ejercerlos todos, como el de limitación al TDP.

Nota: Este es un análisis de la regulación sobre protección de datos personales de otros países de la región con respecto a Ecuador.

Como podemos ver, Ecuador, en comparación con otros países de la región, no contaba ni con un nivel mínimo de protección de datos personales. Los tres países con los que se realizó la comparación se orientan al modelo europeo de protección de datos, por lo cual Ecuador tampoco cumpliría con los niveles de protección que exige la UE. Con esto queda evidenciado que la regulación con la que cuenta nuestro país para la

protección de datos personales no solo es insuficiente, sino que no brinda garantías adecuadas a los titulares de los datos personales. En relación con esto, y tomando en cuenta que la regulación respecto a la TIDP en Ecuador era inexistente, analizamos los proyectos y la ley vigente para verificar si alguna de ellas cumple con algunos de los elementos necesarios para contar con un nivel adecuado de protección para la TIDP.

Propuestas de ley presentadas en Ecuador

Se han presentado tres proyectos de ley para la protección de datos. No obstante, solo el último de ellos, presentado en 2019, cumple con los criterios básicos de una ley de este tipo. Es así que estos proyectos se analizarán para evaluar si cumplen con los estándares de protección analizados en secciones anteriores del libro. Respecto al proyecto de ley de la DINARDAP, el cual se convirtió en la primera ley de protección de datos, se analizará si puede acercar al país a cumplir con un nivel adecuado de protección, con el que se permitan realizar TIDP a un tercer país u organización internacional.

Proyecto de Ley de Protección a la Intimidad y a los Datos Personales

Proyecto presentado por el asambleísta Vethowen Chica el 16 de marzo de 2010. Fue objeto de dos debates, en los cuales se realizaron observaciones que condujeron a su posterior archivo por contener errores sustanciales como: no tener la condición ni el alcance jerárquico de Ley Orgánica, tener errores en creación de acciones para la protección de datos personales, o la creación de un organismo administrativo denominado «Dirección Nacional de Protección de Datos Personales», que en sí no sería una autoridad de control autónoma; o repetir la acción de *hábeas data* como mecanismo para proteger los datos personales. Además, en este proyecto los conceptos de datos personales, datos sensibles, responsables del TDP, eran ambiguos y

no se contemplaba un capítulo para regular la TIDP ni las sanciones por la violación de esta ley.

Proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales

Proyecto presentado por la asambleísta Gabriela Rivadeneira, el 12 de julio de 2016. El primer debate se realizó el 5 de octubre de 2016. Allí se recalcó que la pretensión de este proyecto es proteger los datos personales tanto en el ámbito público como en el privado, puesto que un mal uso de los datos personales pone en riesgo a la esfera de la intimidad y la privacidad de las personas. Además se señaló que los datos personales se vulneran frecuentemente en el ámbito comercial y financiero.

En resumen, este proyecto presentó varias falencias desde su objeto, pues se señala a la intimidad, y luego empeoró en conceptos básicos como: dato personal, responsable del tratamiento de la información; usar la palabra información en vez de dato personal; y al encargado del TDP lo confunde con responsable del archivo, registro, base o banco de datos. No desarrolló correctamente los principios rectores de la protección de datos y dejó de lado el de responsabilidad, licitud y seguridad. Pretende, conforme el artículo 16, que todas las bases o bancos de datos, ficheros o archivos, tanto públicos como privados, con fines exclusivamente financieros y mercantiles, deberían inscribirse en el Registro Nacional de Bases de Datos Personales, vulnerando todo el sentido de la protección de datos personales, ya que el Estado puede tener acceso a todos los datos personales (Enríquez 2017, 56).

En cuanto a la TIDP, no desarrolla cómo se evaluará si un tercer país u organización internacional cuenta con un nivel de protección adecuado, ni posibilita utilizar normas corporativas vinculantes para realizar un TIDP. Como la Autoridad Nacional de Protección de Datos Personales señala a la DINARDAP, adscrita al Ministerio de Telecomunicaciones y de la Sociedad de la Información. Como se señaló, esta autoridad de

control debe ser autónoma, independiente e imparcial, y es cuestionable que la DINADARP sea realmente el órgano adecuado para proteger y ejercer la tutela de los datos personales. Si no contamos con un organismo de control que cumpla con los estándares mínimos para la protección de datos, Ecuador, para el resto del mundo, seguirá sin contar con un nivel adecuado de protección de datos personales.

Ley Orgánica de Protección de datos Personales

La formación del proyecto de ley de la DINARDAP empezó desde 2017. A diferencia de los dos proyectos de ley anteriores, este tuvo la participación de la sociedad civil, la academia, abogados especializados en protección de datos personales, técnicos expertos en seguridad de la información y la cooperación internacional de especialistas en el tema de Colombia y Argentina. Además, por medio de mesas de trabajo, se realizó un acercamiento a las necesidades de cada sector de la sociedad, específicamente del sector público, que juega un doble rol: el de garante del derecho a la protección de datos y el de responsable del tratamiento de ciertos datos. Los objetivos de este proyecto son garantizar el derecho a la protección de datos, promover el libre flujo de información personal, desarrollar la productividad y competitividad del país, e impulsar la innovación y producción nacional.

De esta manera, dos circunstancias demostraron la necesidad de una ley de protección de datos. La primera de ellas ocurrió en septiembre de 2019, cuando periódicos y sitios web internacionales revelaron una filtración de datos que afectó a casi todos los datos personales de los ciudadanos ecuatorianos. La información personal, como números de teléfono, identificación, registros de trabajo, direcciones de domicilio y otras similares, se almacenó en servidores fuera de Ecuador, sin la autorización del interesado. La falta de una ley de protección de datos, que establezca sanciones y medidas correctivas, y una autoridad de protección de datos que las imponga, no permitió tomar medidas inmediatas que hubieran podido evitar que el daño sea más grave.

La segunda circunstancia corresponde a la evolución de las leyes de protección de datos en diferentes países. La llegada del GDPR de la UE, y de otras leyes de protección de datos en todo el mundo, limitan las transferencias internacionales de datos al tiempo que imponen leyes y obligaciones de protección de datos adicionales, que Ecuador no puede cumplir. Así, el proyecto de ley fue presentado el 19 de septiembre de 2019 por parte del entonces presidente de la República del Ecuador, Lenin Moreno. La Comisión de Relaciones Internacionales de la Asamblea Nacional supervisó el análisis y la preparación del proyecto para el primer y segundo debate, a partir de lo cual el 10 de mayo de 2021 fue aprobada por la Asamblea Nacional. La ley debe entrar en vigor en dos años, para que los responsables del tratamiento de datos, hasta ese día, adecúen procesos. Se creará una Superintendencia de Datos, aunque no se establece un plazo máximo para su implementación.

La denominada Ley Orgánica de Protección de Datos Personales (LOPDP) se encuentra estructurada en doce capítulos y setenta y siete artículos, que recogen las tendencias internacionales respecto a la regulación de la protección de datos personales. En el primer capítulo, se establecen disposiciones directivas respecto al objeto, finalidad, ámbito de aplicación material, territorial del proyecto. Además, habla sobre el ámbito de exclusión de la propuesta de ley y ofrece definiciones de los principales conceptos sobre protección de datos. El segundo capítulo trata sobre los principios que rigen el TDP. Allí es evidente la influencia de otras leyes en la materia, como la mexicana y española. No obstante, entre los principios que se destacan, podemos encontrar el de responsabilidad proactiva y demostrada, el cual fue tomado de las Directrices sobre Privacidad de la OCDE y adoptada por el GDPR.

Pese a que la nueva ley de protección de datos era una deuda pendiente del legislador ecuatoriano, hace dos o tres décadas, no es menos cierto que, el hecho de que se lo haya aprobado en 2021 ha permitido que nuestra ley recoja las nuevas tendencias normativas en esta materia y dé, en gran medida, respuesta a las principales inquietudes que plantea un mundo globalizado y tecnificado en el que nos encontramos.

Hay aspectos relevantes a tomar en cuenta; por ejemplo, el ámbito extraterritorial, pues los procesadores y controladores ubicados fuera de Ecuador, que ofrecen bienes y servicios a los residentes ecuatorianos, deben cumplir con las obligaciones de la LOPDP. Sin embargo, no obliga, a quienes realizan el tratamiento de datos, a tener representantes en el país que cumplan con las distintas obligaciones reconocidas en la ley.

En cuanto a la base legal para el tratamiento de datos personales, si bien antes de la ley el ordenamiento jurídico ecuatoriano reconocía, como base legal, el consentimiento, ahora la LOPDP establece obligaciones adicionales, como el interés legítimo, el cumplimiento de obligaciones contractuales y precontractuales, la protección de intereses vitales, el procesamiento de datos almacenados en bases de datos públicas, y el ejercicio de tareas realizadas en interés público o ejercicio de atribuciones públicas.

De igual manera, la nueva ley reconoce los nuevos derechos de los interesados, incluido el de la información, el de acceso, el de rectificación, el de eliminación, el de cancelación, el oponerse, el de no estar sujeto a una decisión basada únicamente en el procesamiento automatizado, el de portabilidad y al olvido. También reconoce excepciones para la aplicación de los derechos de rectificación, supresión, cancelación y oposición. Ellas están relacionadas con la licitud del tratamiento. Además, el derecho al olvido se aplica únicamente a los contenidos digitales. La aplicación del derecho al olvido requiere de la aprobación de un juez. Aun así, no está claro cómo el interesado debe iniciar su reclamo sobre el derecho al olvido.

Los datos sensibles, relacionados con la salud, con los registros financieros y los datos de menores, se consideran categorías especiales de datos personales. Se requiere consentimiento explícito para su tratamiento. Además, tanto los datos de salud como los financieros estarán regulados adicionalmente por leyes específicas.

Sobre las medidas de seguridad, deben implementarlas quienes traten datos personales, y estos deben garantizar la confidencialidad, integridad y disponibilidad de los datos personales. También deben adoptar medi-

das técnicas, según el volumen y tipo de datos tratados. La implementación del análisis de riesgos, la privacidad por diseño y la evaluación del impacto de la protección de datos, son elementos clave para desarrollar un negocio. Además, la ley establece una obligación de notificación, en casos de incumplimientos o filtraciones. En el escenario mencionado, el responsable del tratamiento debe notificar a la autoridad de datos y, en algunos casos específicos, a los interesados.

Es importante recalcar que el responsable del tratamiento y el encargado del tratamiento deben contar con un delegado de protección de datos, según la finalidad, el alcance y la cantidad de datos que se estén tratando. En cuanto a las autoridades públicas, todas deben tener un delegado de protección de datos. Él cooperará con la autoridad de protección de datos y será el punto de contacto con los interesados.

Específicamente, una TIDP se puede realizar a terceros países y territorios cuando estos puedan garantizar un nivel adecuado de protección. La autoridad de protección de datos tendrá una lista de países y territorios que tienen un nivel de protección adecuado. En caso de que la autoridad determine que un país no tiene un nivel adecuado de protección, el procesador o controlador pueden proporcionar las salvaguardas apropiadas. La LOPDP establece los requisitos y condiciones para ello.

La ley crea la Superintendencia de Protección de Datos, como la nueva autoridad de protección de datos. La Superintendencia es una institución autónoma, siguiendo la línea del GDPR. El Superintendente será designado de acuerdo con el procedimiento establecido en la Constitución. A esta autoridad se le ha otorgado la facultad de revisar las actuaciones de los responsables (y encargados) de datos personales de terceros, de que los ciudadanos puedan acudir a ella en caso de que consideren infringidos sus derechos y, asímismo, de que pueda aplicar sanciones a aquellos que incumplan con sus obligaciones.

La LOPDP establece infracciones para el encargado y el responsable del tratamiento, las cuales pueden ser leves o graves y pueden implicar una multa que va del 3% al 17% de sus ingresos anuales del año anterior. La sanción dependerá de la intención (del responsable y del encargado

del tratamiento), reincidencia, gravedad de la infracción, entre otros. Se impondrá después de que se lleve a cabo un procedimiento administrativo.

La nueva ley reconoce algunos principios de gran importancia, a efectos de que el sistema funcione adecuadamente y se eviten abusos, como es el de minimización de datos, que determina que los datos personales deben ser aquellos precisos y limitados específicamente a lo necesario para el cumplimiento de la finalidad del tratamiento. Esto va de la mano con otra concepción importante e innovadora de la ley, que se refiere a la protección de datos por defecto, la cual implica que, en un emprendimiento o proyecto, el responsable aplicará las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines propuestos dentro del proyecto.

Uno de los temas más discutidos fue si había necesidad o no de crear un registro de las bases de datos, que se encontrarían en posesión de los responsables. Esto no quiere decir que se entregue esta información a la Superintendencia para crear una gran base de datos, sino que lo que se entrega responde a fines más bien estadísticos: cuáles son los datos que se están tratando y cuántas bases de datos hay.

En las disposiciones generales, transitorias y derogatorias se busca una adaptación a las demás normas ecuatorianas, pero erróneamente se establece que las medidas correctivas y el régimen sancionatorio se aplicaran dentro de dos años, contados a partir de la entrada en vigor de la ley; pero todo tratamiento de datos realizado antes de esta entrada en vigor debe adecuarse a lo previsto en ella, un criterio confuso que traerá varios problemas de aplicación. No obstante, en general, esta propuesta de regulación, a diferencia de los otros proyectos de ley, mejora bastante en la parte técnica, de redacción y de fondo.

La LOPDP tiene 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, se deben corregir errores, incluir algunas disposiciones y desa-

rrollar ciertas figuras, para regular adecuadamente la protección de datos personales. Con el fin de evidenciar los problemas de las propuestas de ley analizadas, en la siguiente tabla se realiza una comparación, poniendo énfasis en la TIDP.

Tabla 14. Propuestas de ley sobre protección de datos personales en Ecuador

	2010	2016	2019
Correcto ámbito de aplicación territorial	X	X	✓
Conceptos básicos bien desarrollados	X	X	X
Desarrolla correctamente los principios para el TDP	X	X	X
TDP especial para datos personales sensibles	✓	✓	✓
Derechos ARCO	✓	✓	✓
Definición de TIDP	X	X	X
Desarrollo de las TIDP ulteriores	X	X	X
Exigencia de un nivel adecuado de protección para realizar TIDP	✓	X	✓
Declaración de nivel adecuado de protección para realizar TIDP	X	X	✓
Garantías adecuadas para la TIDP	X	X	✓
Normas corporativas vinculantes	X	X	✓
Excepciones para la TIDP	✓	✓	✓
Autoridad de control autónoma	X	X	✓
Mecanismos de certificaciones	X	X	✓
Delegado de protección de datos personales	X	X	✓
Códigos de conducta	✓	X	✓
Obligaciones a los responsables y encargados de los TDP	X	✓	✓
Responsabilidad proactiva y demostrada	X	X	✓

Sanciones administrativas	✓	✓	✓
Sanciones pecuniarias	✓	✓	✓

Nota: Este es un análisis especifico de los temas referentes a la TIDP.

Las propuestas presentadas no cumplen con un nivel suficiente de protección de datos personales, y, menos aún, regulan adecuadamente la TIDP. En cuanto a la LOPDP, mejora notablemente respecto de las dos propuestas anteriores, y a grandes rasgos para regular el TDP cumple con los elementos mínimos necesarios. Sin embargo, hay cuestiones como la definición de dato personal que, a diferencia de otras legislaciones, es bastante complicada, lo que puede producir confusión y tergiversación al momento de determinar qué es un dato personal.

En el marco de la LOPDP, es importante reiterar y considerar la suspensión de las sanciones administrativas (multas y medidas correctivas) que la ley prevé para las empresas y negocios que la infrinjan, y que serán aplicadas por la autoridad de control (en dos años), pues no cambia en dos hechos fundamentales: 1) que las obligaciones ya existen desde la entrada en vigencia de la Ley y, por lo tanto, los incumplimientos ya se pueden registrar, pues las sanciones más graves tienen relación también con la reincidencia, y si alguien incumple ahora –en este período de moratoria–, ya está más cerca de una sanción fuerte, aun cuando su segundo incumplimiento se produzca después; y 2) la suspensión de la sanción administrativa no restringe las otras vías judiciales de las que disponemos ordinariamente; es decir, acciones civiles por daños y perjuicios, acciones constitucionales por vulneración del derecho a la protección de datos personales (con vía en Acción de Protección y Habeas Data), o acciones penales por violación a la intimidad, cuando sea el caso.

En cuanto a la TIDP, la ley no ofrece una definición y no desarrolla adecuadamente las TIDP ulteriores, pero establece tres niveles de protección para realizarla y sus casos excepcionales, lo cual será analizado posteriormente. Respecto al tema de las sanciones, es peculiar, pues para establecer una sanción pecuniaria son muy elevados los porcentajes y se

utiliza el término "volumen del negocio", lo cual produce confusión y no brinda claridad para calcular la sanción. Algo destacable es la autoridad de control. Una Superintendencia, en nuestro ordenamiento jurídico, podría ser la entidad adecuada para proteger y ejercer la tutela de los datos personales, considerando que los estándares internacionales señalan que debe ser un órgano autónomo e independiente.

Nivel adecuado de protección para realizar una TIDP

En este libro se ha evidenciado que la regulación actual sobre protección de datos en Ecuador es insuficiente y en cuanto a la TIDP es inexistente. A partir del análisis de los primeros proyectos de ley, se mostró que no cuentan con un nivel adecuado de protección de datos personales y tampoco ofrecen una regulación completa acerca de la TIDP para que estas se puedan realizar en el país. Los dos proyectos no cumplen con los estándares de protección que se han estudiado en los capítulos previos.

Aun así, el análisis de la LOPDP demostró que, si bien cuenta con ciertas falencias, pretende regular la protección de datos personales de mejor forma que la actual y que la que ofrecían los dos proyectos. Además, respecto a la TIDP, presenta aspectos que requieren de su análisis. Por estas razones, en esta parte, a partir de los estándares de protección para la TIDP estudiados, se exhibirá el nivel en el que se encontraba Ecuador antes y después de la LOPDP. Tomaremos el estándar europeo para realizar el análisis, dado que es el más seguro. Asimismo, consta de tres niveles y un conjunto de excepciones para realizar un TIDP.

Primero, debemos contar con una decisión de la autoridad de control competente, en la que se mencione que ese Estado garantiza un nivel de protección adecuado (este nivel es el más exigente). Ecuador, como hemos visto, no cumple con los elementos que se consideran necesarios para este nivel de protección. Por ejemplo, si bien tiene un respeto por el Estado de Derecho y los derechos humanos, no cuenta con una legis-

lación pertinente en la materia, no tiene una autoridad de control independiente, ni ha adoptado ninguna normativa internacional respecto a la protección de datos.

El segundo nivel ofrece garantías adecuadas, del recuento y análisis de toda la normativa ecuatoriana respecto a la protección de datos personales. Con ello se pudo demostrar que en Ecuador no existe regulación para la TIDP. Por esta razón, no puede aportar las garantías adecuadas por ningún medio, ya que, por un lado, no regula ni da la posibilidad de contar con normas corporativas vinculantes, cláusulas en el tipo de protección de datos ni mecanismos de certificación; y, por otro lado, estos medios deben cumplir con ciertos elementos, los cuales en Ecuador se regulan muy poco. No puede ofrecer aplicación de principios, dar responsabilidad al responsable o encargado del TDP, ni muestra mecanismos o procedimientos de reclamación.

El tercer nivel es realizar una TIDP mediante normas corporativas vinculantes. Como el caso anterior, Ecuador, al no regular nada sobre la TIDP y las normas corporativas, y al no ofrecer una protección adecuada con su normativa, no podría realizar TIDP por medio de estas normas. El último medio por el cual Ecuador puede y realiza TIDP con la UE, Estados Unidos y otros países, es por los casos excepciones, como por medio de un consentimiento explícito del titular de los datos, porque son necesarias para la celebración o ejecución de un contrato y se requieren por el interés público o para proteger los intereses vitales del titular de los datos.

De todas formas, la situación va a variar con la promulgación de la LOPDP. Al estudiarla pudimos ver que regula, de una mejor manera, la protección de datos personales, por lo cual se va a poder realizar una TIDP por cualquier medio antes señalado. Sin embargo, el primer paso, que es contar con un nivel adecuado de protección declarado por una autoridad de control competente, es un tema que quedará pendiente hasta que el país pueda demostrar, a nivel internacional, un conveniente tratamiento de datos personales. Para evidenciar estas afirmaciones, en la siguiente tabla se muestra cómo Ecuador realiza TIDP y cómo, con la aprobación del proyecto, las podría realizar.

Tabla 15. Vías para realizar una transferencia internacional de datos en Ecuador

País o Unión de países	Vías para realizar una TIDP	Vías con las que Ecuador puede realizar una TIDP	
		Antes de la LOPD	Con la LOPD
UE	1. Decisión de nivel adecuado de protección. 2. Garantías adecuadas. 3. Normas corporativas vinculantes. 4. Excepciones.	Excepciones	Nivel adecuado de protección Garantías adecuadas. Normas corporativas vinculantes. Excepciones.
Estados Unidos	1. Normas corporativas vinculantes.	Excepciones	Normas corporativas vinculantes
Argentina	1. Decisión de un nivel adecuado de protección. 2. Excepciones.	Excepciones	Nivel adecuado de protección. Garantías adecuadas. Normas corporativas vinculantes. Excepciones.
México	1. Garantías adecuadas. 2. Normas corporativas vinculantes. 3. Excepciones.	Excepciones	Nivel adecuado de protección. Garantías adecuadas. Normas corporativas vinculantes. Excepciones.
Brasil	1. Decisión de nivel adecuado de protección. 2. Garantías adecuadas. 3. Normas corporativas vinculantes. 4. Excepciones.	Excepciones	Garantías adecuadas. Normas corporativas vinculantes. Excepciones.

Estándar adecuado de protección para realizar una TIDP

En Ecuador, antes de la LOPDP, cuando se realizaba una transferencia internacional de datos, se tenía que recurrir únicamente al consentimiento del titular de los datos, advirtiéndole los riesgos de esta al no poder contar con ninguna de las vías para la TIDP a las que se hizo referencia. Por lo cual, la aprobación de la primera ley de protección de datos personales permitirá realizar una TIDP de maneras más seguras. Para estos efectos, es necesario determinar si los niveles de protección que establecerá la LOPDP, para permitir la TIDP, responden al estándar de protección adecuado que requiere Ecuador. Para lograr este objetivo se tomará en cuenta los beneficios que se puede obtener si el país llega a ser considerado confiable para la TIDP.

Tabla 16. Beneficios de la transferencia internacional de datos

Vías para realizar una TIDP	Países con los que se puede realizar un TIDP	Beneficios
Nivel adecuado	UE, Noruega, Reino Unido, Islandia, Suiza, Uruguay, Argentina, Japón, Canadá, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Nueva Zelanda.	La UE es para Ecuador uno de sus principales socios comerciales con exportaciones de más de 2 000 millones de USD y ahora aún más por el acuerdo comercial firmado en el año 2017. Por esta razón, transferir datos con la UE con un nivel adecuado de protección constituiría una ventaja competitiva.
Garantías adecuadas	México, Colombia, Costa Rica, Panamá, Turquía, Ucrania, Perú, Costa Rica, Australia, Filipinas, Corea del Sur.	Ecuador, mediante convenios internacionales, pretende mejorar la industria nacional, principalmente en el ámbito tecnológico. Lo cual implica crear una normativa interna que pueda adecuadamente proteger los datos personales. Para lograr o mejorar los acuerdos comerciales con estos países, es necesario regular las garantías adecuadas para la TIDP.

Normas corporativas vinculantes	Estados Unidos	Según cifras de la Federación Ecuatoriana de Exportadores (Fedexport), basadas en el Banco Central del Ecuador, las exportaciones a Estados Unidos sumaron 2 536 millones en 2018. Estas cifras demuestran que este país es el principal socio comercial de Ecuador, por lo que la TIDP con Estados Unidos constituye una prioridad.
Casos excepcionales	Venezuela, Jamaica, Rusia, Brasil, Chile, Paraguay, Bolivia, Nicaragua, Honduras, El Salvador, Guatemala, República Dominicana, India, China.	Tanto China como Rusia constituyen mercados atractivos para Ecuador, por lo que transferir datos a estos países podría crear nuevas oportunidades de negocios. De igual forma, la TIDP con países latinoamericanos debe ser una prioridad de Ecuador para fortalecer lazos y relaciones comerciales.

Adaptado de Fedexport 2019, 1-6.

A partir de este análisis, observamos que el estándar de protección adecuado para la TIDP que necesita adoptar Ecuador debe regular las tres vías de protección para realizar una TIDP y los casos excepcionales. Este estándar, al mantenerse apegado a los criterios y principios europeos, servirá para desarrollar el comercio internacional y electrónico con sus principales socios comerciales, pues la nueva ley obliga a empresas y organizaciones a modificar sus procesos internos y prácticas generalizadas, y que conciban a la protección de datos personales como un eje transversal de todas sus actividades y áreas de trabajo.

Por esta razón, la LOPDP estaría regulando adecuadamente la TIDP, ya que toma en cuenta la mayoría de los parámetros a efectos de permitir una de estas transferencias, ocasionando así una libre circulación de datos personales y también garantizando los derechos de los titulares de estos datos. No obstante, como se mencionó, existen algunas deficiencias que deben ser resueltas, como el concepto de dato personal, incluir un concepto de TIDP, desarrollar las TIDP ulteriores y arreglar el régimen sancionatorio para que Ecuador pueda contar con un nivel adecuado de protección.

Si Ecuador quiere obtener beneficios de los intercambios comerciales con Europa y Estados Unidos, del desarrollo de los servicios de la

sociedad de la información, e incrementar su atractivo como país destinatario de TIDP, debe ajustar su ordenamiento jurídico a estándares de protección equivalentes a los que se manejan a nivel internacional, particularmente en Europa. Así lo señala Grande (2016, 69), en virtud de que «[…] en un entorno globalizado como el actual las transferencias internacionales de datos personales resultan imprescindibles no solo a nivel comunitario sino también con relación a terceros países y, en particular, cuando hablamos de Iberoamérica».

A manera de conclusión

A nivel internacional, por los riesgos que implica una TIDP, se ha buscado armonizar los criterios sobre su regulación. Así, podemos establecer un nivel mínimo de protección con el que deben contar los países para poder efectuar una TIDP. La UE y los Estados Unidos son quienes más han desarrollado este tema, por lo que sus modelos de protección de datos personales, a nivel mundial, tienen mayor relevancia. Sin embargo, muestran distintos enfoques: Estados Unidos adopta un enfoque sectorial y de autorregulación, mientras que la UE adopta un enfoque fundamentado en una norma general de aplicación extraterritorial, a más de la exigencia de contar con autoridades de control independientes y niveles adecuados de protección.

La UE, con el GDPR, consiguió implementar el sistema de protección de datos personales más completo, exigente y seguro del mundo. Por ello, varios países y organismos internacionales, como Brasil, México, la APEC y la OCDE, siguen el estándar europeo de protección de datos. El caso de Estados Unidos es particular. Si bien regula la protección de datos, no lo hace adecuadamente. No obstante, dada su importancia, se las arreglado para realizar TIDP, principalmente mediante acuerdos bilaterales, como es el caso con la UE a través del Privacy Shield. Este

acuerdo no cumplió con los elementos y parámetros que exige el GDPR para permitir una TIDP, por lo que en 2020 fue invalidado. Para contrarrestar esto, Estados Unidos, específicamente el estado de California y Nueva York, implementaron en 2020 la CCPA y la SHIELD; normativas, todas ellas, que siguen la tendencia europea en cuanto a la protección 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, sin ellas difícilmente se podría concretar el comercio mundial. Así pues, para evitar los posibles perjuicios a la privacidad de las personas, y para garantizar la libre circulación de datos personales, los Estados han establecido estándares de protección o convenios para regular estas transferencias. Por ejemplo, para que los datos personales puedan ser objeto de transferencias, 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 contar con un nivel adecuado de protección de datos.

Gracias a las constataciones anteriormente expuestas, para garantizar un nivel adecuado de protección para la TIDP, Ecuador debe adoptar el estándar europeo, que consiste en establecer tres vías para realizar las TIDP, y una serie de casos excepcionales. Estas vías exigen el cumplimiento de varios principios, mecanismos, normas y compromisos, que deben cumplir los Estados para autorizar una TIDP. Con el cumplimiento de estos parámetros, en su conjunto, se puede estimar que un país garantiza un nivel de protección de los datos personales, equivalente al brindado por el GDPR.

La regulación sobre protección de datos personales en Ecuador ha sido ineficiente, dado que se encontraba dispersa, incompleta, desactualizada, y era, especialmente, contradictoria. Además, con base en el recuento realizado de la normativa ecuatoriana, la regulación sobre TIDP es inexistente. Por esta razón, se ha propuesto en la asamblea nacional dos proyectos de ley: uno en 2010 y otro en 2016, los cuales, por sus varias deficiencias, no fueron discutidos y aprobados. No obstante, la LOPD

presenta notables mejoras en la regulación de esta materia; aunque, requiere arreglar ciertos problemas para constituirse en una normativa que pueda asegurar un adecuado nivel de protección de datos personales, a la luz del estándar europeo.

La ley protege al ciudadano, que es el deber natural y propio de un Estado; luego, define una serie de reglas que deben ser cumplidas por todos, lo cual otorga seguridad jurídica; ello obliga a los actores, empresas, organizaciones, instituciones públicas, a redefinir y mejorar sus procesos en esta materia, en beneficio de una cultura de protección de datos; permite un mayor flujo de información de datos personales, de forma segura y controlada; plantea menores barreras de entrada a mercados internacionales; facilita las transacciones entre empresas de distintos países. Solo así, Ecuador se convertirá en un destino seguro para receptar datos personales, lo cual es beneficioso para todos.

La promulgación en Ecuador de la LOPDP permitirá regular cómo las empresas nacionales y extranjeras, además de los entes públicos, utilizan, procesan, conservan y explotan los datos personales de las personas naturales en el país. La norma no solo facilita la protección de datos personales, sino también que las empresas tengan bases de datos depuradas y cumplan con estándares homogeneizados a nivel mundial. Es un gran avance para Ecuador. Sin perjuicio de lo anterior, es necesario tener en cuenta ciertos aspectos que no están del todo claros, y podrían causar problemas en el futuro, como: precisar adecuadamente un tratamiento especial a los datos personales sensibles, 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, definir otra forma de cálculo para aplicar las sanciones pecuniarias y corregir los porcentajes del cálculo de estas sanciones.

Referencias

Argentina. Legisalud. Constitución de la Nación Argentina de 23 de agosto de 1994, http://test.e-legis-ar.msal.gov.ar/leisref/public/showAct.php?id=877.

Alexy, Robert. 1993. *Teoría de los derechos fundamentales.* Madrid: Centro de Estudios Constitucionales.

Asamblea Nacional del Ecuador. Proyecto de Ley de Protección a la Intimidad y a los Datos Personales de 2010. 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. Proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales de 2016. 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

Ayalde, Víctor. 2016. «Economía digital: una perspectiva desde el derecho de la competencia.» *Revista Derecho Competencia,* 12. Accedido el 25 de abril de 2020. https://centrocedec. files.wordpress.com/2010/06/5-econom-c3ada-digital.pdf.

Bryan Cave Leighton Paisner LLP. 2018. California Consumer Privacy Act (CCPA). Practical Guide. https://www.bclplaw.com/images/content/1/5/v2/159052/BCLPs-Practical-guide-to-the-CCPA-USA01-12167951.pdf

Bu-Pasha, Shakila. 2017. "Cross-border issues under EU data protection law with regards to personal data protection". *Information & Communications Technology Law,* 3. https://www.tandfonline.com/doi/pdf/10.1080/13600834.2017.1330740?needAccess=true (consultado el 28 de abril de 2020).

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. https://www.icps.cat/archivos/Workingpapers/wp350.pdf?noga=1. (Consultado el 25 de abril de 2020)

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, https://scielo.conicyt.cl/pdf/rdpucv/n36/a09.pdf. (Consultado el 25 de abril de 2020).

Cobb, Stephen. 2019. "GDPR: ¿el primer paso hacia una ley de privacidad global?". *ESET,* , https://empresas.eset-la.com/archivos/novedades/74/Cybersecurity_Trends_2019_v6-ESP.pdf. (Consultado el 25 de abril de 2020)

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. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

Congreso Nacional de Brasil. 2018. Medida Provisional no. 869/18 relativa a la protección de datos personales de 2018, https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062

Colombia. Corte Constitucional. 2011. Sentencia C-748/11 de 6 de octubre de 2011, 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, 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, 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 Tribun al Europeo de Derechos Humanos 2000-II, https://hudoc.echr.coe.int/spa#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-162541%22]}

Cunha, Teresa. 2011. "Las recientes reformas en materia de protección de datos personales en México". *Anuario Jurídico y Económico Escurialense,* núm. 44, https://webcache.googleusercontent.com/search?q=cache:QvlznE2PZ80J:https://dialnet.unirioja.es/descarga/articulo/3625376.pdf+&cd=1&hl=es&ct=clnk&gl=ec. (Consultado el 25 de abril de 2020)

Davara Rodríguez, Miguel. 2006. *Manual de Derecho Informático.* Madrid: Thomson-Aranzadi.

Davara, Isabel. 2011. *Hacia la estandarización de la protección de datos personales: propuesta sobre una "Tercera Vía o Tertium Genus" Internacional.* Madrid: La Ley.

De la Serna, María. 2011. La institucionalización de la protección de datos de carácter personal. En *Reflexiones Sobre el Uso y Abuso de los Datos Personales en Chile,* coordinador Raúl Arrieta, 55-79. Santiago de Chile: Expansiva.

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.

Decreto ejecutivo 864, de 22 de enero de 2016. Reglamento General a la Ley Orgánica de Telecomunicaciones. Suplemento al Registro Oficial 676 de 25 de enero de 2016.

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 de marzo de 2016.

Delpiazzo, Carlos. 2007. "El principio de seguridad jurídica en el mundo virtual". *Revista de Derecho de la Universidad de Montevideo,* 11, http://revistaderecho.um.edu.uy/wp-content/uploads/2012/10/DERECHO-11.pdf. (Consultado el 17 de mayo de 2020)

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

Dirección Nacional de Impresiones y Publicaciones. 2009. Reglamentación de la ley Nro. 18.331, relativo a la protección de datos personales, Uruguay de 2009, Decreto Nro. 414/009, https://www.impo.com.uy/bases/decretos/414-2009

Dirección Nacional de Registro de Datos Públicos. 2019. Proyecto de Ley Orgánica de Protección de datos Personales, https://www.dinardap.gob.ec/wp-content/uploads/downloads/2019/09/PROYECTO-LEY-DE-PROTECCION-DE-DATOS-PERSONALES.pdf

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

----- Código de la Niñez y Adolescencia. Suplemento al Registro Oficial 737 de 3 de enero de 2003.

----- Decreto Ejecutivo 2471, de 11 de agosto de 2005. Reglamento a la Ley Orgánica de Transparencia y Acceso a la Información Pública. Registro Oficial 507 de 19 de enero de 2005.

----- Constitución de la República del Ecuador. Registro Oficial 449 de 20 de octubre de 2008.

----- Código Orgánico Integral Penal. Suplemento al Registro Oficial 180 de 10 de febrero de 2014.

----- Corte Constitucional del Ecuador. Sentencia de jurisprudencia vinculante 001-2014-PJO-CC. Registro Oficial 281, Suplemento, de 3 de julio de 2014

----- Código Orgánico Monetario y Financiero Libro I. Suplemento al Registro Oficial 332 de 12 de septiembre de 2014.

----- Código Orgánico General de Procesos. Suplemento al Registro Oficial 506 de 22 de mayo de 2015.

----- Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación. Suplemento al Registro Oficial 899 de 09 de diciembre de 2016.

----- Decreto Ejecutivo 1156, de 22 de agosto de 2016. Reglamento General a la Ley General de los Servicios Postales. Registro Oficial 854 de 4 de octubre de 2016.

----- Decreto Ejecutivo 111, de 3 de agosto de 2007. Reglamento a la Ley Orgánica de Movilidad Humana. Registro Oficial 55 de 10 de agosto de 2017.

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

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

----- Ley de Seguridad Pública y del Estado, de 2009. Suplemento al Registro Oficial 35 de 28 de septiembre de 2009.

----- Ley de Seguridad Social, de 2001. Suplemento al Registro Oficial 465 de 30 de noviembre de 2001).

----- Ley General de los servicios postales, de 2015. Suplemento al Registro Oficial 603 de 07 de octubre de 2015.

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

----- Ley Orgánica de Gestión de la Identidad y Datos Civiles, de 2016. Suplemento al Registro Oficial 684 de 04 de febrero de 2016.

----- Ley Orgánica de la Salud, de 2006. Suplemento al Registro Oficial 423 de 22 de diciembre de 2006.

----- Ley Orgánica de Movilidad Humana, de 2017. Suplemento al Registro Oficial 938 de 06 de febrero de 2017.

----- Ley Orgánica de Telecomunicaciones, de 2015. Suplemento al Registro Oficial 439 de 18 de febrero de 2015.

----- Ley Orgánica de Protección de Datos Personales, de 2021. Quinto Suplemento al Registro Oficial 459 de 26 de mayo de 2021.

----- Ley Orgánica de Transparencia y Acceso a la Información Pública, de 2004. Registro Oficial 337 de 18 de mayo de 2004.

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

----- Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, de 2018. Registro Oficial 353 de 23 de octubre de 2018.

Estados Unidos de América. Departamento de Justicia. 1966. Freedom of information Act, 5 U.S.C. § 552ª, Ley de libertad de información de 1966, https://www.justice.gov/oip/freedom-information-act-5-usc-552

----- Departamento de Seguridad Nacional. 1974.Privacy Act, 5 U.S.C. § 552ª, Ley de Privacidad de Estados Unidos de Norteamérica de 1974, https://www.uscis.gov

----- Oficina del Asesor Jurídico de Revisión de la Cámara de Representantes. Right to Financial Privacy Act, 12 U.S.C. §§ 3401/342. Ley de libertad de información de 1978, http://uscode.house.gov/view.xhtml?path=/prelim@title12/chapter35&edition=prelim

Enríquez, Luis. 2017. "Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos

a la Intimidad y Privacidad sobre los Datos Personales". *Foro*, núm. 27, http://repositorio.uasb.edu.ec/bitstream/10644/5945/1/05-TC-Enriquez.pdf. (Consultado el 25 de abril de 2020)

Estrada, José, Estrada, Juan, Rodríguez, Ana, y Tipantuña, Christian. 2015. "Ecuador y la Privacidad en Internet: Una Aproximación Inicial". *Revista Politécnica,* núm. 1, https://revistapolitecnica.epn.edu.ec/ojs2/index.php/revista_politecnica2/article/view/556. (Consultado el 25 de mayo de 2020)

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

Eur-Lex. 2019. Caso Schrems vs. Data Protection Commissio ner, sentencia de 6 de octubre de 2015, asunto C-362/14 del Tribunal de Justicia de la Unión Europea, Gran Sala, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62014 CJ0362&from=ES

-----. 2019. Decisión de ejecución, Privacy Shield UE-EE. UU 2016/1250 de la Comisión Europea de 12 de julio de 2020, https://eur-lex.europa. eu/legal-content/ES/TXT/PDF/

----- 2019. Decisión de la Comisión 2000/520/CE, Safe Harbor Privacy Principles de la Comisión Europea de 26 de julio de 2000, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000D0520&from=en

----- 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, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

----- 2019. Reglamento General de Protección de datos del Parlamento Europeo y del Consejo UE 2016/679 de 2016, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Fedexport. 2019. Reporte Mensual de Comercio Exterior. Expordata, http://www.fedexpor.com/wp-content/uploads/2019/02/Expordata-Especial-2018.pdf.

Ferrajoli, Luigi. 2001. Los fundamentos de los derechos fundamentales. Madrid: Trotta.

Foro de Cooperación Económica Asia-Pacífico. 2004. Marco de privacidad de la APEC de 2004, https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

Frosini, Vitorio. 1983. *Los derechos humanos en la sociedad tecnológica.* Madrid: Facultad de Derecho de la Universidad Complutense.

Garrido, Diego. 1991. "El proyecto de Ley de regulación del tratamiento automatizado de los datos de carácter personal: la excepcionalidad como norma". *Jueces para la democracia,* núm. 13, https://dialnet.unirioja.es/descarga/articulo/2528793.pdf. (Consultado el 25 de mayo de 2020)

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,* núm. 27, http://repositorio.uasb.edu.ec/bitstream/10644/5948/1/08-TC-Moritz-Gibello.pdf (Consultado el 25 de mayo de 2020)

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

Gobierno de Brasil. 2018. Ley General de Protección de Datos de Brasil, Nro. 17.309. de 2018, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Gobierno de México. Constitución Política de los Estados Unidos Mexicanos de 5 de febrero de 1917, http://www.sct.gob.mx/JURE/doc/cpeum.pdf

González, Carmen. 2015. Privacidad e historia clínica electrónica la autonomía del paciente y el ejercicio de los derechos ARCO. En *En torno a la privacidad y la protección de datos en la sociedad de la información,* coordinadores J. Aparicio y A. Batuecas, 27-68. Granada: Comares.

Grande, Martha. 2016. "Transferencia internacional de datos personales desde España a países iberoamericanos". *Informática y Derecho,* núm. 1, https://docs.wixstatic.com/ugd/fe8db5_a143e0cda3b44d5998a5c1fe4c70c828.pdf

Gregorio, Carlos. 2005. *Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina.* México: UNAM, https://archivos.juridicas.unam.mx/www/bjv/libros/3/1407/12.pdf

Guasch Portas, Vicente. 2012. "La transferencia internacional de datos de carácter personal". *Revista de Derecho UNED*, 11, 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

Infoleg. Reglamentación de la ley Nro. 25.326, relativo a la protección de datos personales de Argentina de 2001, Decreto Nro. 1558/2001, http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/texact.htm

Levin, Avner. y Nicholson, Mary. 2005. "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground". *University of Ottawa law & technology journal,* 357, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=894079. (Consultado el 25 de mayo de 2020)

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, https://www.uria.com/documentos/publicaciones/5315/documento/art03.pdf?id=6965. (Consultado el 25 de mayo de 2020)

Lucena, Isabel. 2012. "La protección de la intimidad en la era tecnológica: hacia una reconceptualización". *Revista Internacional del Pensamiento Político*, 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, https://scielo.conicyt.cl/pdf/revider/v30n1/art04.pdf. (Consultado el 25 de mayo de 2020)

México. Honorable Cámara de Diputados. Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México de 2010, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

----- México. Honorable Cámara de Diputados. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de México de 2017, http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

----- México. Honorable Cámara de Diputados. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México de 2011, http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

Naranjo, Lorena. 2017. "El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador". *Foro,* núm. 27, http://repositorio.uasb.edu.ec/bitstream/10644/5946/1/06-TC-Naranjo.pdf. (Consultado el 25 de mayo de 2020)

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*, núm. 27, http://repositorio.uasb.edu.ec/bitstream/10644/5947/1/07-TC-Ordo%C3%B1ez.pdf. (Consultado el 25 de mayo de 2020)

Organización de Estados Americanos. Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la OCDE de 1980, http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf

Ley de Protección de Datos Personales de Argentina, Nro. 25.326 de 2000, https://www.oas.org/juridico/PDFs/arg_ley25326.pdf

Ornelas, Lina. 2008. Transferencias internacionales de datos personales: su protección en el ámbito del comercio internacional y de seguridad nacional. En *Procesos constitucionales de la libertad,* coordinadores E. Ferrer y A. Zaldívar, 731-758. México: Marcial Pons.

Ortega, Alfonso. 2017. "Transferencia Internacional de Datos de Carácter Personal: del Safe Harbour al Privacy Shield". *Lex Mercatoria,* núm. 4, http://revistas.innovacionumh.es/index.php?journal=lexmercatoria&page=article&op=view&path%5B%5D=1093&path%5B%5D=208. (Consultado el 25 de mayo de 2020)

Ortega, Alfonso, y Juan Domenech. 2018. "Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea". *Re-*

vista de la Facultad de Derecho, núm. 44, https://dx.doi.org/10.22187/rfd2018n44a2. (Consultado el 25 de mayo de 2020)

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

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

Pulido, Carlos. 2015. Derechos fundamentales. En *Enciclopedia de filosofía y teoría del derecho,* editado por Jorge Fabra y Alvaro Nuñez, 1571-1594. México: UNAM.

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

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

Red Iberoamericana de Protección de Datos. 2017. Estándares de protección de datos personales para los Estados Iberoamericanos de la RIPD de 2017, http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

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,* núm. 16, https://revistas.javeriana.edu.co/index.php/internationallaw/article/view/13847 (Consultado el 25 de mayo de 2020)

Remolina, Nelson. 2015. *Recolección internacional de datos personales: un reto del mundo post-internet,* Madrid: España.

Rojas, Marcela. 2014. "Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales". *Novum Jus,* núm 8, https://editorial.ucatolica.edu.co/ojsucatolica/revistas_ucatolica/index.php/Juridica/article/viewFile/652/670. (Consultado el 25 de mayo de 2020)

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

Sánchez Gonzáles, M. 2015. Implicaciones Institucionales de la Ley de Protección de Datos. Tesis Doctoral. Universidad de Málaga, https://riuma.uma.es/xmlui/bitstream/handle/10630/11792/TD_SANCHEZ_GONZALEZ_Maria_Belen.pdf?sequence=1&isAllowed=y

Sánchez, Alvaro. 1998. *La protección del derecho a la libertad informática en la Unión Europea».* Sevilla: Universidad de Sevilla, Secretariado de Publicaciones.

Santos, Juan. 2013. "The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon". *CLEER Working Papers,* núm. 2, https://www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf. (Consultado el 25 de mayo de 2020)

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.

Torres, Bolívar. 2010. Proyecto de Ley Orgánica de Protección de Datos Personales. Tesis de maestría. Universidad de Cuenca, http://dspace.ucuenca.edu.ec/bitstream/123456789/2660/1/tm4350.pdf

Tribunal Constitucional Español. Sentencia 292/2000 del Tribunal Constitucional Español de 30 de noviembre de 2000, http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276#complete_resolucion&completa

Uicich, Rodolfo. 1999. *Los bancos de datos y el derecho a la intimidad.* Buenos Aires: AD-HOC.

Uría, Elisa. 2016. "Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems". *Revista de Derecho Comunitario Europeo,* núm. 53, http://dx.doi.org/10.18042/cepc/rdce.53.07. (Consultado el 25 de mayo de 2020)

Uruguay. Dirección Nacional de Impresiones y Publicaciones. 2008. Ley de

Protección de Datos Personales de Uruguay, Nro. 18.331 de 2008, https://www.impo.com.uy/bases/leyes/18331-2008

Valverde, Antonio. 2013. "Protección de datos de carácter personal y derechos de información de los representantes de los trabajadores". *Temas Laborales, núm.* 118, http://www.juntadeandalucia.es/empleo/anexos/ccarl/33_1392_3.pdf. (Consultado el 25 de mayo de 2020)

Villalba, Andrea. 2017. "Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa". *Foro,* núm. 27, http://repositorio.uasb.edu.ec/bitstream/10644/5944/1/04-TC-Villalba.pdf. (Consultado el 25 de mayo de 2020)

Warren, Samuel, y Louis Brandeis. 1890. "The Right to Privacy". *Harvard Law Review, núm.* 5, http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (Consultado el 25 de mayo de 2020)

Brasil. World Intellectual Property Organization. Constitución de la República Federativa de Brasil. 5 de octubre de 1988, https://www.wipo.int/edocs/lexdocs/laws/es/br/br117es.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

Anexos

Anexo 1. Desarrollo normativo de la protección de datos personales en Ecuador.

Cuerpo Normativo	Ámbito de regulación	Aspectos relevantes
Constitución Política del Ecuador (1998)	Reconoce el derecho a la intimidad, establece acción de *hábeas data*, prohíbe la utilización de información personal salvo para necesidades de atención médica y señala que se debe establecer en la ley un procedimiento especial para acceder a datos personales que consten en archivos relacionados con la defensa nacional.	Señala como derechos civiles en el art. 23 a: el derecho a la honra, a la buena reputación y a la intimidad personal y familiar (Núm. 8). El derecho a guardar reserva sobre sus convicciones. Que en ningún caso se podrá utilizar la información personal de terceros sobre sus creencias religiosas y filiación política, ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades de atención médica (art. 21). Señala en el art. 94 que toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito, que es la acción de *hábeas data*.
Ley de Seguridad Social (2001)	Regula el sistema nacional de seguridad social y hace referencia al registro de datos personales de los trabajadores asegurados.	El registro de historia laboral del asegurado comprenderá los datos personales del asegurado (art. 274). Además, señala que la información de la historia laboral del asegurado es reservada.
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos (2002)	Su ámbito de regulación radica a los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos.	Establece que para usar o transferir datos personales necesariamente se requiere la autorización del titular o la orden de autoridad competente (art. 9, inciso 1). Señala que la recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución y esta ley (art. 9, inciso 2). Define a los datos personales como: aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley (Glosario).

Código de la Niñez y Adolescencia (2003)	Regula la protección legal a los Niños, Niñas y Adolescentes.	Conforme el art. 30, núm. 3 se debe mantener registros individuales en los que conste la atención y seguimiento del embarazo, el parto y el puerperio; y registros actualizados de los datos personales, domicilio permanente y referencias familiares de la madre. En cuanto a la mediación señala que el Consejo de la Judicatura llevará un registro cuantitativo y sin datos personales del adolescente y sus familiares (art. 348-C).
Ley Orgánica de Transparencia y Acceso a la Información Pública (2004)	Regula el ejercicio del derecho fundamental a acceder a la información.	Se considera información confidencial aquella referente a lo público personal, que no está sujeta al principio de publicidad. Comprende aquella derivada de sus derechos personalísimos y fundamentales (art. 6).
Reglamento a la Ley Orgánica de Transparencia y Acceso a la Información Pública (2005)	Regula la aplicación de las normas de la Ley Orgánica de Transparencia y Acceso a la Información Pública.	Señala que una de las causales para interponer el Recurso de Acceso a la información es que la información sea considerada incompleta, alterada o supuestamente falsa (art.16).

Ley Orgánica de la Salud (2006)	Regular las acciones que permitan efectivizar el derecho universal a la salud consagrado en la Constitución Política de la República y la ley (art. 1).	Es responsabilidad del Ministerio de Salud Pública regular y vigilar la aplicación de las normas técnicas para la detección, prevención, atención integral y rehabilitación, de enfermedades transmisibles, no transmisibles, crónico-degenerativas, discapacidades y problemas de salud pública declarados prioritarios, y determinar las enfermedades transmisibles de notificación obligatoria, garantizando la confidencialidad de la información (art. 6, núm. 5). Toda persona tiene en relación con la salud, el derecho a tener una historia clínica única redactada en términos precisos, comprensibles y completos; así como la confidencialidad respecto de la información en ella contenida (art. 7, lit. f). Según el Art. 211 es obligatorio guardar confidencialidad respecto al genoma individual de la persona el cual es un dato personal.

Constitución de la República del Ecuador (2008)	Reconoce el derecho a la protección de datos personales. Desarrolla la acción de *Hábeas Data*. Señala que mantendrá la confidencialidad de los datos de carácter personal que se encuentren en los archivos de las instituciones de Ecuador en el exterior (art. 44).	Confidencialidad de los datos personales de las personas ecuatorianas en el exterior, cualquiera que sea su condición migratoria (art. 40). Reconoce el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (art. 66, núm. 19). El Art. 66, núm. 20 reconoce el Derecho a la intimidad. Según el art. 92 toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.
Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009)	Regula la jurisdicción constitucional y la forma de garantizar la eficacia y la supremacía constitucional.	Desarrolla en el art. 49 el objeto de la acción de *hábeas data* que es garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas, en soporte material o electrónico. Asimismo, señala que toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, origen y destino, y el tiempo de vigencia del archivo o banco de datos.

Ley de Seguridad Pública y del Estado (2009)	Regula la seguridad integral del Estado, la seguridad ciudadana y la soberanía e integridad territorial. Respecto a los datos personales prohíbe recolectarlos sin un fin lícito.	En el art. 22 se indica que ningún organismo de inteligencia está facultado para obtener información, producir inteligencia o almacenar datos sobre personas, por el solo hecho de su etnia, orientación sexual, credo religioso, acciones privadas, posición política o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción.
Ley Orgánica del Sistema Nacional de Registro de Datos Públicos (2010)	Crea y regula el sistema de registro de datos públicos y su acceso, en entidades públicas o privadas que administren dichas bases o registros (art. 1).	Señala que los datos personales sensibles son confidenciales y tienen una protección especial (art. 6, inciso 1). El acceso a estos datos solo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial (art. 6, inciso 2). Establece los principios de consentimiento, licitud, seguridad y finalidad para el acceso a los datos sensibles (art. 6, inciso 4).
Código Orgánico Integral Penal (2014)	Establece los delitos que lesionan el derecho a la protección de datos personales.	Señala que la persona privada de libertad tiene derecho a la protección de sus datos de carácter personal (art. 12). Delito de violación a la intimidad (art. 178). Delito de revelación ilegal de base de datos (art. 229).

Código Orgánico Monetario y Financiero Libro I (2014)	Regula los derechos de los usuarios financieros, las prohibiciones a las entidades del sistema financiero, la protección de la información, del sigilo y reserva de la información y sus excepciones y el Registro de Datos crediticios y el acceso de su titular a este registro.	Señala que es derecho de los usuarios financieros que la información y reportes crediticios que sobre ellos constan en las bases de datos de las entidades financieras sean exactos y actualizados con la periodicidad establecida en la norma (art. 152). Se prohíbe a las entidades del sistema financiero comercializar las bases de datos de sus clientes (art. 235, núm. 18). Los datos de carácter personal de los usuarios del sistema financiero nacional que reposan en las entidades de dicho sistema y su acceso están protegidos, y solo podrán ser entregados a su titular o a quien este autorice o por disposición de este Código (art. 352). El Registro de datos crediticios es utilizado únicamente para fines de análisis crediticio. Otro uso se encuentra prohibido (art. 360).
Código Orgánico General de Procesos (2015)	Regula la actividad procesal en todas las materias, excepto la constitucional, electoral y penal, con estricta observancia del debido proceso (art. 1).	Las y los juzgadores garantizarán que los datos personales de las partes procesales se destinen únicamente a la sustanciación del proceso y se registren o divulguen con el consentimiento libre, previo y expreso de su titular (art. 7).
Ley General de los servicios postales (2015)	Regula y controla la administración y gestión de los servicios postales. Protege los datos de los usuarios de estos servicios.	Una de las obligaciones de los operadores postales es: proteger los datos de los usuarios; por tanto, no podrán facilitar ningún dato relativo a la existencia del envío postal, a su clase, a sus circunstancias exteriores, a la identidad del remitente y del destinatario, ni sus direcciones, salvo pedido expreso de autoridad competente o judicial (art. 34, núm. 13). Es derecho de los usuarios de los servicios postales recibir igualdad de trato y confidencialidad de sus datos, aun cuando para el control se usen técnicas o medios electrónicos o informáticos (art. 35, núm. 11).

Ley Orgánica de Telecomunicaciones (2015)	Regula el régimen general de telecomunicaciones y del espectro radioeléctrico.	Establece el derecho de los abonados, clientes u usuarios a la privacidad y protección de sus datos personales, por parte del prestador con el que contrate servicios (art. 22, núm. 4). Señala la Obligación de los prestadores de servicios de telecomunicaciones de adoptar las medidas necesarias para la protección de los datos personales de sus usuarios y abonados (art. 24, núm. 14). Los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y de gestión adecuadas para garantizar la protección de datos personales (Principio de consentimiento y seguridad, debido TDP, derecho de acceso, deber de información, arts. 78, 79 y 82).
Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos (2016)	Desarrolla y aplica las disposiciones previstas en la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos (art. 1).	Señala los principios por los que se debe regir todo tratamiento de datos públicos, como: principio de calidad de datos, finalidad, utilidad, incorporación, rectificación, responsabilidad y seguridad (art. 11). Consagra los derechos de rectificación, actualización, eliminación y anulación de datos públicos (art. 12).
Reglamento General a Ley Orgánica de Telecomunicaciones (2016)	Regula la aplicación de la Ley Orgánica de Telecomunicaciones.	Reafirma que los prestadores de servicios del régimen general de telecomunicaciones tienen prohibido ejecutar u omitir acciones que violen la garantía de protección de datos personales (art. 120).
Reglamento General a la Ley General de los Servicios Postales (2016)	Mide la aplicación de la ley que regula los servicios postales y establece que los operadores postales deberán brindar una protección de los datos personales de los usuarios de este servicio.	Los operadores postales no podrán usar datos personales de sus usuarios para ningún otro fin que la prestación de los servicios postales (art. 7, inciso 1). La obligación de protección de los datos incluirá el deber de secreto de los datos personales, la confidencialidad sobre el contenido e información de los envíos y la protección de la intimidad (art. 7, inciso 4).

Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación (2016)	Regula el Sistema Nacional de Ciencia, Tecnología, Innovación y Saberes Ancestrales. En cuanto a los datos personales se los trata en la ética, en la investigación científica, en las bases de datos producto de las investigaciones científica, en la utilización de datos personales o no personales en contenidos protegidos o no por propiedad intelectual.	En la investigación científica se debe cumplir con ciertos ámbitos, uno de ellos es la confidencialidad de los datos personales (art. 67, núm. 5). Utilización de datos personales en contenidos protegidos o no por propiedad intelectual:) Cuando se trate de información clasificada como asequible; b) Cuando cuenten con la autorización expresa del titular de la información; c) Cuando estén expresamente autorizados por la ley; d) Cuando estén autorizados por mandato judicial u otra orden de autoridad con competencia para ello; y, e) Cuando lo requieran las instituciones de derecho público para el ejercicio de sus respectivas competencias o del objeto social para el que hayan sido constituidas (art. 141). El tratamiento de datos personales que incluya acciones tales como la recopilación, sistematización y almacenamiento de datos personales, requerirá la autorización previa e informada del titular a menos que sea realizado por una institución pública para fines estadísticos o científicos (Disposición General Vigésima Séptima).
Ley Orgánica de Gestión de la Identidad y Datos Civiles (2016)	Regula la inscripción, registro y modificación de los hechos y actos relativos al estado civil de las personas y su identificación.	En el art. 75 establece que se necesita autorización del titular para acceder a archivos físicos o electrónicos de la Dirección General de Registro Civil, Identificación y Cedulación que estén sujetos al principio de confidencialidad y publicidad.
Ley Orgánica de Movilidad Humana (2017)	Regula el derecho a la confidencialidad de las personas ecuatorianas en el exterior, personas con protección internacional y refugiados.	Señala que las personas ecuatorianas en el exterior tienen derecho a la confidencialidad de sus datos de carácter personal, cualquiera sea su condición migratoria (art. 7) Confidencialidad de los datos de las personas en protección internacional y que el acceso a los datos personales se realizará por autorización de la persona titular de la información o con orden de autoridad judicial competente (art. 94). El procedimiento de determinación de la condición de refugiado respetará el principio de confidencialidad y la protección de los datos personales en todas sus etapas (art. 99).

Reglamento a la Ley Orgánica de Movilidad Humana (2017)	Regula la aplicación de la Ley Orgánica de Movilidad Humana y la confidencialidad de los datos personales de todo refugiado.	Todo refugiado y solicitante de dicha condición tiene derecho a la protección y confidencialidad de sus datos personales (art. 78).
Reglamento a la Ley Orgánica de Gestión de la Identidad y Datos Civiles (2018)	Regula la aplicación de Ley Orgánica de Gestión de la Identidad y Datos Civiles.	Define a los datos personales como aquellos que permiten identificar o volver identificable a una persona natural (art. 2, núm. 5). Indica que cuando se registre datos personales sensibles la autoridad competente deberá implementar los niveles de protección de datos personales más adecuados para proteger los derechos de las personas (art. 93).
Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos (2018)	Regula la optimización de trámites administrativos, su simplificación y reduce sus costos de gestión.	Señala que las y los administrados tienen el derecho a acceder a los registros, archivos y documentos de la Administración Pública. Pero, se excluyen aquellos que involucren datos personales de terceros o tengan la calidad de confidenciales o reservados, excepto cuando la información tenga relación directa con la persona y su acceso sea necesario para garantizar su derecho a la defensa (art. 5). Queda prohibida la cesión o transferencia de datos personales de ciudadanos no involucradas con la prestación del servicio por parte de personas naturales o jurídicas del sector privado que sean gestoras, delegadas o concesionarias de un servicio público que no cuenten con el consentimiento del titular de los datos (art. 11).

Nota: Es la normativa ecuatoriana que regulaba la protección de datos personales.

La transferencia internacional de datos personales en Ecuador
Protección frente al libre flujo

se terminó de editar
en Quito, Ecuador,
en el mes de noviembre del 2021.
bajo la marca

udla
ediciones
siendo canciller el Dr. Carlos Larreátegui Nardi

Pre- es un afijo que se antepone a una palabra para cambiar su significado. De ahí que esta colección exhiba los trabajos de titulación de alto valor académico con lo que los estudiantes graduados de pregrado, acceden a un nuevo escalón profesional.

Este libro inaugura esta colección

Otras colecciones de UDLA Ediciones

La protección de datos no ha sido una prioridad en el ordenamiento jurídico ecuatoriano. Si bien la Constitución de Montecristi reconoce el derecho a la protección de datos, hasta 2020 no se había creado una ley específica sobre los alcances y obligaciones en materia de protección de datos. Esta falta de desarrollo normativo limita la posibilidad de transferencia internacional de datos, puesto que estas imponen obligaciones que Ecuador no podía cumplir. Históricamente otras legislaciones han mostrado una mayor preocupación por la protección de datos, como es el caso de la Unión Europea que, en 2016, con el Reglamento General de Protección de Datos, estableció un marco regulatorio que elevó el nivel de protección que los Estados deben proporcionar para garantizar el derecho a la protección de datos. Por esta razón, Estados Unidos ha tenido que buscar mecanismos con los cuales hacerle frente al estándar europeo de protección de datos, y Latinoamérica intenta actualizar y promulgar legislaciones sobre esta materia. El presente trabajo analiza las similitudes y diferencias de los mecanismos jurídicos de protección de datos de ciertos países de América, la Unión Europea y de las organizaciones internacionales, que cuentan con instrumentos normativos sobre transferencia internacional de datos, como la APEC y la OCDE. Por último, con esta información se argumenta cómo Ecuador, con su nueva ley de protección de datos, debe afrontar de manera adecuada los desafíos que representa la transferencia internacional de datos personales.

ISBN: 978-9-9427-7932-8
9 789942 779328