FACULTAD DE DERECHO Y CIENCIAS SOCIALES

ESTÁNDAR ADECUADO DE PROTECCIÓN PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES EN EL ECUADOR

AUTOR

Christian Alejandro Razza Sandoval

AÑO

2019

FACULTAD DE DERECHO Y CIENCIAS SOCIALES

ESTÁNDAR ADECUADO DE PROTECCIÓN PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES EN EL ECUADOR

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Abogado de los Tribunales y Juzgados de la República

Profesor Guía

Mgs. Lorena Naranjo Godoy

Autor

Christian Alejandro Razza Sandoval

Año

2019

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido el trabajo, Estándar adecuado de protección para la transferencia internacional de datos personales en el Ecuador, a través de reuniones periódicas con el estudiante Christian Alejandro Razza Sandoval, en el semestre 201920, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Lorena Naranjo Godoy

Magíster en Derecho de las Nuevas Tecnologías

CC:170829378-0

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado el trabajo, Estándar adecuado de protección para la transferencia internacional de datos personales en el Ecuador, del estudiante Christian Alejandro Razza Sandoval, en el semestre 201920, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Rafael Eduardo Serrano Barona
Magíster en Derecho Energético y Recursos Naturales
CC: 171298093-5

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____

Christian Alejandro Razza Sandoval

CC: 171817037-4

AGRADECIMIENTOS

La culminación de este trabajo es gracias al ejemplo y compromiso de mis padres, Isabel y William, mi eterna gratitud hacia ellos. Son mi fuerza y mi inspiración.

No habría podido lograr tanto si el apoyo constante de toda mi familia, Sarahí, Any, Mama, Marquito y Andre, gracias.

Mi profundo agradecimiento a los docentes que han formado parte de mi formación profesional, en especial, a los Doctores Lorena Naranjo y Rafael Serrano, quienes con su conocimiento y guía hicieron esto posible.

DEDICATORIA

A mi familia, especialmente a mis padres por todo el sacrificio que han hecho y por todo el apoyo que me han brindado para que pueda cumplir con todas mis metas.

RESUMEN

Los datos personales se han vuelto a nivel internacional un activo intangible que permite la productividad y competitividad. Razón por la cual se ha visto necesario que se regule adecuadamente su tratamiento por una serie de mecanismos, derechos y principios que garanticen el derecho a la protección de datos personales. En la actualidad este derecho se lo concibe como un derecho autónomo, complejo e instrumental. El Ecuador, con la Constitución del 2008 lo reconoció, sin embargo, hasta ahora no ha brindado las garantías suficientes para efectivizar su protección. Aún más grave, es que no existe regulación respecto a la transferencia internacional de datos personales (TIDP), por lo cual si los datos personales de sus ciudadanos son objeto de una de estas transferencias se encontrarían en un total estado de desprotección. Históricamente algunas legislaciones han mostrado una preocupación mayor por la protección de datos personales, como es el caso de la Unión Europea (UE) que, en el 2016, con el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) estableció un conjunto de mecanismos para la TIDP.

Por esta razón, en la UE con el GDPR se exige un nivel adecuado de protección a terceros países u organizaciones internacionales, a efectos de autorizar una TIDP. Tendencia que se ha ido siguiendo a nivel mundial, en Estados Unidos con el *Privacy Shield,* y en Latinoamérica con la adopción y aplicación de estándares internacionales en sus legislaciones específicas sobre protección de datos personales. En esta línea, en la presente investigación conforme el estudio de los estándares de protección que se manejan a nivel internacional, específicamente en Europa y Estados Unidos, se determinará cual estándar de protección le conviene adoptar al Ecuador si quiere favorecerse de los beneficios que implica una adecuada regulación en cuanto a la TIDP.

Palabras clave: estándar, dato personal, protección de datos personales, transferencia internacional de datos personales.

ABSTRACT

Personal data has become an intangible asset internationally that allows productivity and competitiveness. Reason why it has been necessary to regulate its treatment properly by a series of mechanisms, rights and principles that guarantee the right to the protection of personal data. At present, this right is conceived as an autonomous, complex and instrumental right. Ecuador, with the 2008 Constitution recognized it, however, until now it has not provided enough guarantees to make effective its protection. Even more serious, is that there is no regulation regarding the international transfer of personal data (ITPD), so if the personal data of its citizens are subject to one of these transfers would be in a total state of vulnerability. Historically some legislations have shown a greater concern for the protection of personal data, as is the case of the European Union (EU) which, in 2016, with the General Data Protection Regulation (GDPR) established a set of mechanisms for ITPD.

For this reason, in the EU with the GDPR an adequate level of protection is required from third countries or international organizations, in order to authorize an ITPD. Trend that has been followed worldwide, in the United States with the Privacy Shield, and in Latin America with the adoption and application of international standards in their specific legislation on personal data protection. In this line, in the present investigation according to the study of the protection standards that are handled internationally, specifically in Europe and the United States, it will be determined which protection standard suits to adopt Ecuador if it wants to advantage from the benefits implied by an adequate regulation regarding the ITPD.

Keywords: standard, personal data, protection of personal data, international transfer of personal data.

ÍNDICE

INTRODUCCIÓN 1

1 CAPÍTULO I. PROTECCIÓN, TRATAMIENTO Y TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES 3

1.1 El dato 3

1.2 Datos personales 4

1.3 Protección de datos personales 6

1.3.1 Fundamento de la protección de datos personales 8

1.3.2 Configuración actual del derecho fundamental a la protección de datos personales 9

1.3.3 Principios rectores 11

1.4 Tratamiento de datos personales (TDP) 13

1.5 Transferencia internacional de datos personales (TIDP) 15

1.5.1 Definición y alcance 15

1.5.2 Sujetos intervinientes 16

1.5.3 Principios propios de la TIDP 17

1.5.4 Importancia 19

2 CAPÍTULO II. ESTÁNDARES PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES 20

2.1 Estados Unidos de América 21

2.1.1 De la *Fredoom of Information Act (*FOIA*)* a la *Right to Financial Privacy Act* (RFPA) 21

2.1.2 Del *Safe Harbour* al *Privacy Shield* 23

2.1.3 *California Consumer Privacy Act* (CCPA) 27

2.2 Unión Europea (UE) 29

2.2.1 Antecedentes 30

2.2.2 Reglamento General de Protección de Datos (GDPR) 33

2.3 Referentes de América Latina en la regulación de la protección de datos personales 37

2.3.1 República de Argentina 37

2.3.2 Estados Unidos Mexicanos 38
2.3.3 República Federativa del Brasil 40
2.3.4 Estándares de protección de datos personales para los Estados Iberoamericanos (2017) 41
2.4 Organizaciones internacionales que regulan los flujos transfronterizos de datos personales 42
2.4.1 La Organización para la Cooperación y el Desarrollo Económicos (OCDE) 42
2.4.2 Foro de Cooperación Económica Asia-Pacífico (APEC) 43
2.5 Comparación entre las regulaciones sobre la TIDP 44
3 CAPÍTULO III. ESTÁNDAR ADECUADO DE PROTECCIÓN PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES EN EL ECUADOR 46
3.1 Situación actual de la protección de datos personales en el Ecuador 48
3.2 Propuestas de ley presentadas en el Ecuador para regular la protección de datos personales 52
3.3 Niveles de protección adecuados para realizar una TIDP 57
3.4 Estándar de protección adecuado para realizar TIDP en el Ecuador 59
4 CONCLUSIONES 62
REFERENCIAS 65
ANEXOS 83

ÍNDICE DE TABLAS

Tabla 1. Principios rectores de la protección de datos personales 11

Tabla 2. Definiciones sobre el tratamiento de datos personales 13

Tabla 3. Principales instrumentos normativos que protegen los datos personales en Estados Unidos 23

Tabla 4. Comparación entre el Privacy Shield y el Safe Harbour 26

Tabla 5. Comparación entre el GDPR y la CCPA 28

Tabla 6. Antecedentes normativos de la protección de datos personales en la UE 30

Tabla 7. Niveles de protección para realizar una TIDP 34

Tabla 8. Comparación entre la Directiva 95/46/CE y el GDPR 36

Tabla 9. Comparación entre la normativa sobre protección de datos personales en América Latina 42

Tabla 10. Comparación con respecto a la protección de datos personales 45

Tabla 11. Comparación general respecto a la TIDP 45

Tabla 12. Desarrollo normativo de la protección de datos personales en el Ecuador 48

Tabla 13. Comparación entre Ecuador y otros países latinoamericanos respecto a la protección de datos personales 51

Tabla 14. Comparación entre las propuestas de ley que se han presentado en el Ecuador respecto a la protección de datos personales y la TIDP 56

Tabla 15. Comparación entre los niveles de protección para la TIDP 59

Tabla 16. Niveles adecuados de protección para la TIDP y sus beneficios económicos 60

INTRODUCCIÓN

La época actual se caracteriza por una actividad social, cultural, económica, jurídica y política que constantemente rebasa fronteras. Los avances tecnológicos se han fundido con nuestro diario vivir y prácticamente todas las áreas de la sociedad se ven afectadas por la tecnología. El avance tecnológico ha permitido que el tráfico de información se realice rápidamente y en grandes cantidades, lo cual, en ocasiones, se constituye como una herramienta para facilitar el comercio y el desarrollo de las sociedades, y otras veces, un riesgo para los derechos de las personas (Rebollo y Serrano, 2017, pp. 21-23).

En la sociedad de hoy, la información tiene un precio muy alto. Por esta razón, el tratamiento de esta información debe ser regulada por el Derecho para evitar la violación de derechos fundamentales. El tratamiento de datos personales (TDP) debe estar concebido para servir a la humanidad, por eso en el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) de la Unión Europea (UE) en el considerando 4, no se concibe al derecho a la protección de datos personales como un derecho absoluto, sino en relación con su función en la sociedad y para mantener el equilibrio con otros derechos. Además, debido al desarrollo de la tecnología y el aumento de la transferencia internacionales de datos personales (TIDP) ya no se debe pensar en restringir sino en controlar el tratamiento de estos datos.

En este contexto el Ecuador, como parte de la economía mundial, se ve expuesto a múltiples presiones, tanto políticas como económicas, las cuales están relacionadas con la protección de datos personales y la TIDP. Lo cual, constituye un desafío para el Derecho, por una parte, por la necesidad de equilibrar el interés público que puede existir respecto a estos datos y, por otra, para velar por el respeto a los derechos fundamentales de la persona propietaria de dicha información. Así pues, la ausencia de criterios internacionales uniformes en el Ecuador acerca de la protección para la TIDP no solo dificulta la relación con dos de sus más importantes aliados comerciales, Estados Unidos y la UE, sino que

además “acentúa las diferencias conceptuales entre los diversos sistemas de derechos humanos, cuya característica fundamental debe residir precisamente en su universalidad.” (Maqueo, Moreno y Recio, 2017, p. 93).

En relación con lo anterior, el Ecuador en el año 2017 suscribió un Acuerdo Comercial con la UE, que además de contener temas relacionados al comercio, establece ciertos parámetros para la protección de los derechos humanos, ya que entiende que lo primero no puede justificar el menoscabo de lo segundo. La inexistencia en el Ecuador de un nivel adecuado de protección para la TIDP, aun reconociendo en el Art. 66, núm. 19 de la Constitución de 2008 el derecho a la protección de datos personales dificulta la relación con la UE toda vez que ha ocasionado un incumplimiento del Acuerdo restándole de esta manera competitividad comercial al país en la esfera internacional.

En este sentido, el problema jurídico que se pretende resolver en el presente trabajo se resume en la siguiente pregunta de investigación: ¿Cuál es el estándar adecuado de protección con el que debería contar el Ecuador para la TIDP? Sobre este problema jurídico, se defenderá en la presente investigación la posición de que: el Ecuador para la TIDP requiere adoptar y aplicar los estándares de protección para la TIDP que se sigue a nivel internacional, como el europeo o norteamericano. De tal forma, para el desarrollo de este trabajo se utilizará varios métodos de investigación, tales como: la exégesis, para analizar las diversas normas internacionales que regulan la TIDP y el método analógico para determinar los estándares internacionales sobre protección de datos que siguen la mayoría de los Estados y como estos se pueden aplicar en el Ecuador.

Por consiguiente, para resolver esta problemática la presente investigación se encuentra dividida en tres capítulos. El primero, trata los conceptos generales sobre la protección de datos personales, haciendo hincapié en su tratamiento y la TIDP. El segundo, se enfoca en analizar los dos principales modelos de protección para la TIDP existentes: el estadounidense y el europeo, adicionando un estudio de las principales organizaciones internacionales que han emitido

regulaciones sobre la TIDP y como estos han sido aplicados en América Latina. El tercero, partiendo de un análisis de la situación actual del Ecuador respecto a la TIDP y con las bases obtenidas de los capítulos previos se determinará cuál es el estándar adecuado de protección con el que el Ecuador debe contar para la TIDP; y, por ende, garantizar que estas transferencias se realicen respetando los derechos y garantías establecidas en la Constitución y los cambios regulatorios ocurridos en el derecho comparado durante los últimos años. Al final, en las conclusiones, se presenta de manera resumida los principales resultados de la investigación.

1 CAPÍTULO I. PROTECCIÓN, TRATAMIENTO Y TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

La tecnología ha permitido, entre otras cosas, diluir la noción de fronteras territoriales, lo cual amplia el ámbito de actuación de las empresas e insta a los Estados adaptar su legislación a estos cambios. En este nuevo contexto global donde diariamente se intercambia datos personales implica una problemática para el Derecho, el cual debe brindar los mecanismos legales apropiados para proteger los derechos de las personas. De tal manera, en este primer capítulo, se desarrollará la conceptualización y caracterización de los datos personales, el derecho a la protección de datos, el TDP y la TIDP. Adicionalmente, se hará referencia a los principios, sujetos intervinientes y la importancia de la TIDP.

La información de las personas en la actualidad se ha vuelto imprescindible para la realización de toda clase de actividades e iniciativas públicas y privadas, por ende, resulta importante proteger esta información para que no existan abusos ni vulneración de derechos (Sánchez, 1998, p. 26). De tal manera, para entender la importancia de la protección de los datos personales en la TIDP, se debe partir de la noción de dato.

1.1 El dato

Cualquier discusión sobre la protección de datos debe tener una idea clara del significado de los términos "información" y "dato" que, aunque puedan parecer términos sinónimos, no lo son. Autores como González (2015, p. 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, p. 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 realizan 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, la cual para Naranjo (2017, p. 73) “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 con el GDPR se utiliza el término “dato” porque se considera a este concepto lo suficientemente amplio para abarcar todo tipo de información. Lo que Uicich (1999, p. 40) reafirma al indicar que el dato, aunque parezca irrelevante o inocuo por el avance tecnológico un TDP está en la capacidad de formar un perfil con solo ese dato. Así pues, por la importancia y cuidado que requieren los datos personales surge la necesidad de regular su tratamiento.

1.2 Datos personales

Los datos personales pueden ser tan sencillos como los nombres y apellidos, o pueden ser complejos como los datos biométricos, o tan sensibles como los datos de salud. Los datos personales son una lista extensa y abierta, que va creciendo, como el número de seguro social, los datos genéticos y hasta

nuestros *likes* en *Facebook*. En realidad, en el mundo actual hay miles de formas en las que nuestro propio día a día nos hace identificables (Gil, 2016, p. 45).

El dato personal 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) definen al dato personal como "toda información relativa a un individuo identificado o identificable". Similares conceptos de dato personal se encuentran en el derecho comparado, por ejemplo, en el Art. 2 de la ley argentina de protección de datos personales donde se conceptualiza a los datos personales 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.". Lo cual, el Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE en su Dictamen número 4/2007 y el GDPR en su Art. 4 punto 1 acogen en su definición de dato personal. De estas definiciones se puede destacar los siguientes elementos: cualquier información, sobre, persona física e identificada o identificable.

El elemento "toda información" o "cualquier información" se puede considerar bastante amplio. Para autores como Zaballos (2013, p. 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 ofrecer 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, p. 68). Por lo cual, se realiza una descripción amplia de modo que se pueda acoger todo tipo de datos personales.

Según el Art. 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 a la sexualidad. De tal manera, 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” se refiere a que la información debe ser concerniente y relacionarse directamente con una persona física. Se excluye la protección de datos personales relativos a personas jurídicas, aunque en el derecho comparado se puede 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 esa persona debe indicar a quién le pertenece, sin necesidad de realizar una investigación posterior (Gil, 2016, p. 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. En virtud de que en varias ocasiones los datos personales son utilizados para fines ilícitos sus titulares deben contar con los medios adecuados para proteger su privacidad.

1.3 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, p. 88). Sus respectivas doctrinas son las bases más relevantes para el desarrollo de la protección de datos personales en todo el mundo. En Estados Unidos la protección de datos personales, en sus inicios se fundamentó en el derecho a la privacidad, cuyo desarrollo tiene como origen la doctrina de *Privacy Law* desarrollada por Samuel Warren y Louis Brandeis en 1890. En Europa, en

cambio, las ideas norteamericanas fueron sustituidas por la doctrina de la autodeterminación informativa que consiste en el derecho de cada persona a determinar en qué medida se puede comunicar a otros sus datos personales, idea creada por Alan Westin en 1967 que da inicio al desarrollo de la materia en Europa (Lucena, 2012, p. 129). Al respecto de esto se indica que:

> "El 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" (Torres, 2010, p. 9).

La protección de datos personales surgió debido a los avances tecnológicos que permitieron conectar al mundo en tiempo real, para resguardar el derecho a la privacidad de las personas. Sin embargo, con el tiempo llegó a ser un mecanismo jurídico que otorga a la persona el control y disposición de todos sus datos (Sanz, 2008, p.139). Por ello, Enríquez (2017, p. 44) señala que los objetivos principales de la protección de datos son: establecer que 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 el Ecuador a partir de Constitución del año 2008 se establece a la protección de datos como un derecho de libertad de todos los ciudadanos, lo que de manera similar sucede en otros países de Latinoamérica. Por consiguiente, a continuación, se explicará concretamente que abarca la protección de datos personales y en que se fundamenta.

1.3.1 Fundamento de la protección de datos personales

Para comprender lo que engloba la protección de datos y entender su fundamento se debe señalar al derecho a la intimidad como su fuente primigenia. Sin embargo, posteriormente se separa 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, p. 65). Su concepto ha variado según el contexto en el que fue desarrollado en Estados Unidos en su primera aproximación se lo concebía como correlativo al *Right to Privacy*, mientras que en Europa se concibe como un derecho autónomo frente al derecho a la intimidad y privacidad.

Para Frosini (1983, pp. 101-110) el derecho a la intimidad se concibe como un conjunto de facultades que permiten la exclusión de injerencias de terceros en la esfera íntima de la persona. Según Delpiazzo (2007, p. 11) la protección de datos personales transitó desde un sentido negativo hacia un sentido positivo, en el cual 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. De tal forma, aunque algunos datos personales parezcan insustanciales estos pueden permitir la formación de perfiles y, por ende, replicar en 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 indicó que la protección de datos personales tiene una naturaleza autónoma, ya que se concibe como una garantía del titular de los datos personales a como disponer de estos datos, cualquiera sea su naturaleza y no solo los que forman parte de su intimidad. De tal manera, el objeto de la protección de datos no se reduce a los datos íntimos de la persona, es mucho más amplio, alcanza incluso los datos personales públicos. Consecuentemente, constituye una protección a la persona ante la manipulación o injerencia no autorizada por la ley, de sus datos personales.

1.3.2 Configuración actual del derecho fundamental a la protección de datos personales

La protección de los derechos fundamentales ha variado a lo largo del tiempo, no siempre se ha concedido el mismo nivel de protección ni se ha reconocido los mismos derechos fundamentales. Estos surgen para dar solución a las necesidades cambiantes de la sociedad, por ejemplo, el derecho a la protección de datos personales nació 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 como el derecho a la protección de datos personales, que partió como una garantía a la vida privada, luego paso a ser entendida como el derecho a la autodeterminación informativa, y, finalmente, como un derecho autónomo.

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

> “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, consiste en un conjunto de propiedades formales y materiales (Pulido, 2015, pp. 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, de saber el contenido, uso y destino de la información contenida en estos ficheros (Guzmán, 2013, p. 114). Asimismo, este derecho tiene un carácter instrumental frente a otros derechos reconocidos, por un lado, porque 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, ya que el uso indebido de datos personales puede afectar otros derechos, como el de educación o salud (Puccinelli, 1999, p. 68).

El derecho a la protección de datos personales otorga a la persona facultades positivas de disposición y control de sus datos, a diferencia del derecho a la privacidad que confiere facultades negativas de exclusión a terceros de la vida privada de una persona (Remolina, 2015, p. 89). En palabras del Tribunal Constitucional Español en la sentencia 292/2000 consiste en “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 cuales se pueden establecer limitaciones, por ejemplo, la TIDP. “El ciudadano de un Estado social de Derecho no tiene un derecho absoluto e ilimitado sobre sus datos, sino que por ser parte de un conglomerado tiene que aceptar limitaciones en aras del interés superior” (Garriga, 2016, p. 94). Los datos son necesarios para realizar varias actividades lícitas, legítimas y de interés general o particular, por eso no es un derecho para oponerse al tratamiento, sino para exigir uno correcto (Remolina, Tenorio y Quintero 2018, p. 48).

En síntesis, el derecho a la protección de datos personales es un derecho autónomo, pues protege toda tipo de datos de carácter personal y no sólo 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, p.38). Su contenido conlleva, una pluralidad de derechos básicos, principios y garantías lo que lo convierte en un derecho complejo (Valverde, 2013, p. 21). De tal modo, para su efectivo ejercicio debe incluir tanto el acceso a la información, como la posibilidad de actualizar, rectificar, eliminar u oponerse, de esto resultan los derechos denominados ARCO necesarios para un adecuado TDP que ahora con el GDPR aumentaron también el derecho a la portabilidad de los datos, limitación del tratamiento y el derecho al olvido.

1.3.3 Principios rectores

El derecho a la protección de datos personales se garantiza mediante la previsión en la ley de una serie de mecanismos y elementos dirigidos a asegurar el control y el dominio sobre los datos. Con el fin de preservar este derecho fundamental se necesita aplicar una serie de principios y criterios específicos para su tratamiento (Sanz, 2008, p. 139). De acuerdo con Alexy (1993, p. 458) los principios son mandatos de optimización, normas que ordenan la realización de algo en la medida de las posibilidades jurídicas y reales. En diferentes instrumentos jurídicos internacionales se ha 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 los que la mayoría de las legislaciones sobre protección de datos ha tomado de modelo. A continuación de manera sistematizada, se desarrollará 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, p. 276). El TDP tiene que hacerse, siempre con apego a la normativa aplicable y conforme lo acordado entre el responsable del tratamiento	RIPD (2017), GDPR (2016), OCDE (2013), APEC (2004), Ley de protección de datos de: Argentina (2000), México (2017), Brasil (2018).

	y el titular de los datos personales a través de los medios permitidos por la norma.	
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 que 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, p. 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 poder obtener, en cualquier momento y sin restricciones información acerca de la existencia, como se trata y cualquier otra información sobre los datos que le conciernan (Monsalve, 2016, p. 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, p. 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, p. 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 sólo 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, p. 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, p.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." como lo indica (Remolina et al., 2018, p. 62). Deben ser mantenidos durante no más tiempo del 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, p. 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, p. 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 “de estar en la capacidad de demostrar que el interesado otorgó su consentimiento para el tratamiento de los datos de carácter personal.” (Quesada, 2017, p. 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.

1.4 Tratamiento de datos personales (TDP)

El TDP se ha convertido en una actividad cotidiana y de alta importancia para el Estado, las empresas y los particulares. Todos requieren de información personal para tomar y ejecutar decisiones de diversa naturaleza (económica, seguridad nacional, política, laboral, financiera, comercial, entre otros). El TDP rebasa fronteras, debido a la globalización de las actividades, como el comercio electrónico. Por este motivo, 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 ha expedido a nivel mundial un sin número de normas generales y sectoriales. La regulación del TDP no se opone al uso de datos sino a su eventual abuso toda vez que el TDP puede llegar a provocar una vulneración de los derechos humanos de los titulares de los datos (Remolina et al., 2018, p.48). Con esta introducción, ahora corresponde señalar que se debe entender por TDP, por su importancia varias organizaciones y países lo definen de distintas maneras, en la siguiente tabla se expondrá las más significativas:

Tabla 2.

Definiciones sobre el 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 también 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 más 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 se puede extraer que el TDP puede ser automatizado o no. La expresión “tratamiento de datos personales” debe ponerse en relación con la de base de datos, en virtud de que los datos personales deben estar contenidos dentro de una base de datos, que según el Art. 4 numeral 6 del GDPR es todo conjunto estructurado de datos personales, accesibles, centralizado o descentralizado. Conforme el Art. 4 del GDPR son 3 las partes que participan en un TDP. (1) El interesado que es la persona física cutos 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. (3) El encargado es la persona física o jurídica, de naturaleza pública o privada que trate datos distinta de la persona responsable o lleve a cabo un TDP por cuenta del responsable del TDP.

Con respecto a las fases del TDP autores como Davara Rodríguez (2006, p. 69) y Zaballos (2013, p. 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 si existe comunicación, cesión o transferencia ya que los datos salen del responsable o encargado hacia

un tercero. Adicionalmente, una forma en la cual se puede dar un TDP es a través de una TIDP, por lo cual a continuación se la desarrollará.

1.5 Transferencia internacional de datos personales (TIDP)

En 1980 la OCDE en sus directrices señalaba que la TIDP se ha incrementado considerablemente en años recientes y van a aumentarse con el desarrollo de las tecnologías y las comunicaciones. De Terwangne (2009, p.177) explica que en los procesos de integración económica existe la necesidad de exportar e importar datos personales entre las empresas privadas, las personas o las autoridades de los diferentes países. Estos procesos como el incremento de las relaciones comerciales internacionales y sociales hicieron necesario expedir normas sobre el TDP que conciliaran la protección de la privacidad y la TIDP. La TIDP fue una de las principales razones que motivaron la regulación sobre TDP. “La transferencia internacional de datos forma parte del ¿qué? y del ¿por qué? se quería regular y armonizar la protección de datos.” (Remolina, 2015, p.150).

1.5.1 Definición y alcance

Conforme el GDPR y la sentencia Lindqvist vs. Gäta hovärtt., Del Tribunal de Justicia de la Unión Europea (TJUE), una TIDP se produce cuando los datos personales que son tratados por un responsable o un encargado de un TDP que se encuentra en el Espacio Económico Europeo son enviados fuera de dicho territorio a un tercer país u organización internacional. De forma más amplia la TIDP es (Grande, 2016, p. 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 Art. 4 literal h) del Decreto No. 414/009 reglamentario a 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 ubicados en un Estado y que son enviados a otros Estados.

La TIDP se puede dar por motivos muy variados, 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, p. 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. 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 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 sobre protección de datos la TIDP puede poner en riesgo los derechos de las personas. Sin embargo, como señala Castellanos (2017, p. 6) sin la TIDP difícilmente se podría dar el comercio mundial. Así pues, para evitar los posibles perjuicios que a la privacidad de las personas podría causar una TIDP y 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.

1.5.2 Sujetos intervinientes

De las definiciones expuestas, es posible identificar en la TIDP la participación de dos partes: el exportador de datos y el receptor de los datos personales. Con 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. De tal forma, en una TIDP tenemos dos personas: 1) el exportador, definido en el Art. 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 Art. 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: a) dos responsables del tratamiento, por ejemplo, uno establecido en el España y otro establecido en un tercer país o ser una organización internacional, b) un responsable y un encargado del tratamiento, encontrándose el responsable, por ejemplo, establecido en Estados Unidos y el encargado del TDP en Francia, o c) dos encargados del TDP, uno asentado en Argentina y otro en Brasil.

1.5.3 Principios propios de la TIDP

Para que los datos personales puedan ser objeto de TIDP a más de cumplir con los principios rectores para la protección de datos, se debe tomar en consideración los principios de continuidad de la protección y el principio de equivalencia necesarios para poder contar con un nivel adecuado de protección para la TIDP. A continuación, se desarrollará estos principios.

a) Principio de continuidad de la protección

Un estándar adecuado de protección no puede implicar una disminución de la protección con la que ya contaban los datos personales en el país de origen de la persona titular de los datos cuando estos son transferidos internacionalmente. Al respecto, De Frutos en 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 contaban en el país de origen de los datos. Se busca que el nivel de protección del país exportador se garantice en el país importador.

b) Principio de equivalencia

A nivel internacional no todos los Estados ofrecen las mismas garantías en cuanto a la protección de datos personales; por ejemplo, en Europa se cuenta con amplia legislación y jurisprudencia sobre el tema, mientras que en países como Ecuador, Venezuela y Bolivia todavía no se cuenta con una ley de protección de datos. Por esta falta de uniformidad entre los países diferentes legislaciones e instrumentos jurídicos internacionales (GDPR*,* la legislación de Argentina, México, Brasil, las Directrices de la OCDE y el *Privacy framework* de la APEC) exigen para autorizar una TIDP que el país receptor de datos deba contar con un nivel de protección equivalente al que ofrece el país emisor, en términos de Remolina (2010, p.497) para una TIDP se debe verificar que el país importador garantice un nivel de protección de los datos personales adecuado.

El exigir un nivel adecuado de protección para autorizar una TIDP constituye el principio de equivalencia que tiene como fin 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, p. 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.”.

1.5.4 Importancia

Para Remolina (2010, p. 493) la TIDP que no se encuentre debidamente regulada y reglada es un problema por tres principales razones: (1) Disminuye la protección jurídica de la información, pone al titular de los datos en un estado de vulnerabilidad al no tener como proteger sus datos. (2) Constituye una situación desventajosa en el contexto comercial, restándole competitividad al país porque imposibilita su participación en transacciones comerciales internacionales que involucren TIDP perjudicando directamente a los empresarios (Garrido, 1991, p. 17). (3) La protección de datos se relaciona con el concepto de sociedad democrática, la falta de ella implica una afectación al sistema político que sostiene el Estado de Derecho.

Para Ornelas (2008, p. 147) un régimen que regule adecuadamente la TIDP implica contar con una regulación equilibrada que facilite el comercio internacional y a la vez proteja los datos personales. De tal modo, los beneficios que obtiene un país al contar con un nivel adecuado de protección para la TIDP son principalmente 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 tiene 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 al comercio entre las partes. La UE es una de las mayores economías mundiales y una importante fuente y beneficiaria de inversión extranjera. De tal forma, el Ecuador para no incumplir con el acuerdo y mejorar sus relaciones con la UE debe adoptar un estándar adecuado de protección de datos para lograr garantizar seguridad a los titulares de los datos cuando estos son transferidos.

En síntesis, el derecho a la protección de datos personales se fundamenta en proteger al titular de los datos, debido a lo que un TDP inadecuado de un simple

dato suyo, como su nombre puede ocasionar. Por los avances tecnológicos el comercio internacional es una realidad que requiere de una gran cantidad de transferencia de datos personales. Así pues, por los riesgos y posibles efectos negativos que puede causar una TIDP en los derechos de las personas, es que a nivel internacional se ha buscado armonizar su regulación, de modo que se garantice en todos los lugares del mundo un nivel adecuado de protección de datos personales cuando se realice una TIDP. De tal forma, los siguientes capítulos de la presente investigación se enfocarán en profundizar sobre la regulación de la TIDP a nivel mundial y de qué forma el Ecuador debe adecuarse a esta regulación para contar con un nivel adecuado de protección para la TIDP.

2 CAPÍTULO II. ESTÁNDARES PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

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

En este segundo capítulo, por la fuerte incidencia en la regulación internacional para la TIDP que tienen el modelo americano y europeo, se realizará su análisis para determinar el estándar de protección de datos personales con el que se manejan. Adicionalmente, se estudiará como en América Latina se está regulando la TIDP, tomando como referencia a Argentina, México y Brasil; y, por

último, se analizará las regulaciones para la TIDP que han emitido los organismos internacionales como la OCDE y el APEC.

2.1 Estados Unidos de América

En Estados Unidos el derecho a la protección de datos personales tiene como antecedente principal, el derecho a la privacidad o *Right to Privacy*. Esta doctrina construida por Louis Brandeis y Samuel Warren en 1890 aportó con una reinterpretación de los precedentes en la materia ya que, hasta ese 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, p. 275). Con esta nueva interpretación 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, p. 14). En Estados Unidos en el siglo XX se dictaron tres leyes que establecen los principios rectores que configuran el derecho a la privacidad en este país: la *Fredoom of Information Act* (FOIA) de 1966, la *Privacy Act* de 1974 y la *Right to Financial Privacy Act* (RFPA) de 1978. En el siglo XXI aparecieron el *Safe Harbor* de 2000 y posteriormente el *Privacy Shield* de 2016 para regular la TIDP con Europa, y la *California Consumer Privacy Act* (CCPA) de 2018 que entrará en vigor en 2020. A continuación, se analizarán las leyes mencionadas.

2.1.1 De la *Fredoom of Information Act (*FOIA*)* a la *Right to Financial Privacy Act* (RFPA)

Si bien la *Privacy Act* de 1974 fue una de las primeras protecciones para evitar un inadecuado uso de los datos personales por parte del gobierno, es la FOIA la que establece primero el derecho al acceso de los datos almacenados por los organismos públicos. Conforme esta Ley, la administración pública está obligada a tener listados actualizados que permitan al público conocer el tipo de información contenida en cada registro de cada organismo del Estado. Con la FOIA las personas tienen el derecho solicitar en instancias judiciales el acceso a su información que se encuentre en los registros de las agencias federales.

La *Privacy Act* la cual, tiene por objeto regular la recopilación, mantenimiento, uso y difusión de la información personal que figuran en bancos de datos del gobierno federal (Sánchez González, 2015, p. 174). Constituyo una de las primeras y más importantes regulaciones del uso de los datos personales por parte del gobierno, pero su alcance es limitado, ya que sólo aplica al procesamiento de datos por parte del gobierno federal y no aplica a los gobiernos estatales ni al sector privado. (Levin y Nicholson, 2005, p.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 y para investigaciones del Congreso (Gregorio, 2005, p. 307).

En el año 1978 se promulgo la RFPA, la cual, fue diseñada para proteger la confidencialidad de los registros financieros personales, pero sólo del gobierno (Levin y Nicholson, 2005, p.364). La RFPA entrega a las personas confidencialidad 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 ámbito de regulación de estas leyes son:

Tabla 3.

Principales instrumentos normativos que protegen los datos personales 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 mantienen en un sistema de registros bajo el control de una agencia federal.	Otorga los derechos de acceso, rectificación y el derecho de 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, pp. 174-175); (Levin y Nicholson, 2005, pp.362-365).

Nota: principales aspectos regulatorios de estas leyes.

Por consiguiente, la FOIA, la *Privacy Act* y la RFPA supusieron hitos en el desarrollo del derecho a la privacidad en Estados Unidos. Pero, al solamente tener un ámbito de regulación público, no llegaron a constituirse de la forma en la que se lo había planeado. En cuanto a la TIDP, en estas leyes no se hace mención ni se las regula.

2.1.2 Del *Safe Harbour* al *Privacy Shield*

En el Art. 25 de Directiva 95/46/CE del Parlamento Europeo y del Consejo se señalaba que la TIDP a terceros países se realice solamente cuando el tercer país garantice un nivel de protección adecuado. En el apartado 6 se establecía que la Comisión Europea (CE) podrá hacer constar que ese país garantiza el 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 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, p. 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 efectuada desde la UE a Estados Unidos al cumplimiento de los Principios de Puerto Seguro anexo I de la Decisión, los cuales 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, p. 7).

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

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

facultaba a las empresas y organizaciones de la UE a realizar TIDP a Estados Unidos (López, 2017, p. 36).

En los fundamentos de hecho de la Sentencia, Maximillian Schrems, de nacionalidad austriaca, que era usuario de la red *Facebook* desde 2008, presentó una reclamación ante el *Data Protection Commissioner* el 25 de junio de 2013 solicitando que prohibiera a *Facebook Ireland* transferir sus datos personales a Estados Unidos toda vez que este país no garantizaba una protección suficiente de los datos personales conservados en su territorio. Schrems, además, hizo referencia a las revelaciones que Edward Snowden hizo en 2013 sobre las actividades de los servicios de información de Estados Unidos, en particular las de *las National Security Agency*.

Según los fragmentos (del 70 al 89) de la sentencia del caso *Schrems vs. Data Protection Commissioner* 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 garantiza un nivel adecuado de protección conforme 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. (5) Los procedimientos legales para exigir el cumplimiento de los principios son limitados.

Posterior a la publicación de la Sentencia del caso *Schrems* mediante la Declaración del Grupo de Trabajo del artículo 29 de 16 de octubre de 2015 hubo un llamado a toda la comunidad europea a buscar soluciones jurídicas, políticas y técnicas que permitan la TIDP a los Estados Unidos. En la señalada Declaración se instó a las instituciones europeas y a los Estados a iniciar urgentemente negociaciones con Estados Unidos para conseguir una solución antes del 31 de enero de 2016 y tal como lo explica Uría (2016, p. 280) justo “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), N.º 2016/1250, de la CE, de fecha 12 de julio de 2016 se acordó el *Privacy Shield* con el que, se permitió de nuevo realizar TIDP desde la UE a los Estados Unidos sin necesidad de abordar la autorización de la entidad de control (Castellanos, 2017, p. 26). Su contenido se compone por una serie de principios que vienen consagrados en los Anexos I y II de la Decisión, los cuales, en sentido amplio se estructuran, en siete principios generales y dieciséis que los complementan. Acorde con el objetivo esta investigación, a continuación, se realizará una comparación entre 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 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 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: 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 sobre el TDP y permitir la TIDP con la UE. Estos marcos regulatorios son su estándar de protección para realizar la TIDP con la UE. No obstante, el *Safe Harbour* que fue

el marco regulatorio que más tiempo estuvo vigente, aunque fue acogido por miles de empresa americanas, no era de carácter obligatorio, no estaba en igual rango que otras leyes americanas y se encontraba desactualizado, lo cual dificultaba su aplicación y, por ende, tuvo que ser sustituido. El *Privacy Shield* si bien entro a cubrir los vacíos de su antecesor sigue cayendo en los mismos problemas, no es un marco regulatorio obligatorio y no implica que Estados Unidos sea un país con un nivel adecuado de protección de datos personales.

2.1.3 *California Consumer Privacy Act* (CCPA)

La CCPA es una ley de privacidad del consumidor que se aprobó en el Estado de California el 28 de junio de 2018. Desde que se encontraba como proyecto de ley ha sido descrita como el GDPR en los Estados Unidos, de hecho, esta ley es la legislación de privacidad más fuerte promulgada en cualquier Estado hasta el momento. Como se verá a continuación, otorga más poder a los consumidores en lo que respecta a sus datos privados. Dada la variedad de gigantes tecnológicos con sede en California, como *Google* y *Facebook*, la CCPA está preparada para tener efectos de gran alcance en la privacidad de los datos personales desde el 1 de enero de 2020 cuando entre en vigor.

Con el CCPA se pretende otorgar 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 divulga 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. Por la importancia del tema, se ha señalado que en los próximos años otros Estados seguirán el ejemplo de la CCPA, apegándose cada vez más a los estándares de GPDR (Cobb, 2019, p. 18). De tal modo, las empresas americanas que tomen medidas proactivas hoy, para proteger mejor los datos de los consumidores estarán mejor preparadas para enfrentar las olas de cambio (Bryan Cave Leighton Paisner LLP, 2018, pp. 7-13). Dada la relación de esta nueva Ley con el GDPR se realizará una comparación entre 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, p. 2).

Nota: diferencias entre el GDPR y el CCPA.

En resumen, la protección de datos en Estados Unidos se ha seguido orientado a través de los años por un modelo de autorregulación, que no es eficiente y no garantiza 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 no ofrecen y no cumplen con los debidos estándares de protección como para garantizar adecuadamente el derecho a la protección de datos personales. La CCPA que sigue la tendencia del GDPR muestra por la importancia del Estado de California la orientación que probablemente sigan los demás Estados.

2.2 Unión Europea (UE)

La regulación sobre protección de datos personales a menudo escapa de la esfera de los Estados y transciende a nivel internacional. En Europa, después de la II Guerra Mundial, se sintió la necesidad y la obligación de defender los derechos humanos, y con la cooperación entre sus países, se creó la primera organización internacional en el continente, el Consejo de Europa (CE), con el Tratado de Londres el 5 de mayo de 1949 (Cerda, 2011, p. 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 dicho convenio incorporado a su legislación nacional. El derecho a la protección de datos personales encuentra cabida en el Art. 8 del CEDH.

Posteriormente, por los riesgos que el desarrollo de la tecnología podría implicar para los derechos fundamentales, desde comienzos de los años setenta, los Estados comenzaron a emitir normativa sobre protección de datos personales y 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 la protección de datos directamente tuvo el objetivo de proteger la privacidad ante las nuevas tecnologías (De la Serna, 2011, p. 60). Pero, en 1981, el CE adoptó unos 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 considerarse la primera norma europea que marcó las pautas del modelo común de protección de datos personales con el que se maneja Europa hasta la actualidad (Remolina, 2010, p. 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, se realizará un recuento de los instrumentos jurídicos más importantes sobre 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.

2.2.1 Antecedentes

La regulación sobre protección de datos personales en la UE ha venido desarrollándose a lo largo del tiempo con gran interés debido a que, 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, es donde radica la importancia del derecho a la protección de datos personales, ya que permite proteger en estos intercambios de datos personales los derechos de los titulares de estos datos (Rojas, 2014, p. 110). En la UE desde el Convenio 108 de 1981 se ha emitido varias normas comunitarias que regulan la protección de datos personales, por lo que en la siguiente tabla se mostrará el panorama normativo de la UE sobre esta materia.

Tabla 6.

Antecedentes normativos de la protección de datos personales en la UE

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) No 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, p. 112).

Nota: desarrollo normativo en la UE sobre protección de datos personales.

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

De la mano con la regulación normativa sobre protección de datos personales, en la UE hubo un importante desarrollo jurisprudencial. Uno de los más importantes es la sentencia 209/83 dictada por el Tribunal Constitucional Federal Alemán el 15 de diciembre de 1983 sobre el censo de 1982. En la sentencia por primera vez se concibió al derecho a la protección de datos personales como un derecho autónomo e independiente del derecho a la vida privada e instituyó el primer paso para la construcción y desarrollo del derecho. Para declarar a la protección de datos personales un derecho autónomo 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 sobre cómo debe ser tratada su información, en términos de este tribunal:

> “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.” (Tribunal alemán, 1983, Sentencia 209/83).

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 cual se elaboró la Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al TDP y a la libre circulación de estos datos. Posteriormente, se destaca el reconocimiento explícito del derecho a la protección de los datos personales en la Carta de los Derechos Fundamentales de la UE, de 7 de diciembre del 2000, documento que 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, a efectos de cumplir con las obligaciones que imponía este Directiva, 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, p. 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, p. 22).

La Directiva 95/46/CE, se encontraba estructurada en 7 Capítulos, en los cuales establecía su objeto; definía términos esenciales; delimitaba su ámbito de aplicación; indicaba las condiciones generales para la licitud del TDP, se hacía referencia a los principios del derecho a la protección de los datos personales y los derechos de que gozan los titulares de los datos objeto de tratamiento; señalaba los recursos judiciales, responsabilidad y las sanciones; regulaba la TIDP; explicaba la elaboración de Códigos de Conducta; trataba sobre la Autoridad de Control; y, hablaba sobre las medidas de ejecución comunitarias.

Respecto al presente tema de investigación, en el Capítulo IV de la Directiva 95/46/CE se regulaba la TIDP, donde 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 flujos de datos hacia terceros países. El carácter adecuado del nivel de protección se evaluada por la CE mediante una Decisión de Adecuación, considerando diferentes criterios tales como: la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, el ordenamiento jurídico vigente en el país tercero de que se trate, las normas profesionales y las medidas de seguridad en vigor en dichos países, todo esto conforme al Art. 25 de la Directiva 95/46/CE. Criterios que se aumentaron con la promulgación del GDPR en 2016.

2.2.2 Reglamento General de Protección de Datos (GDPR)

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 a fin de reformar la normativa ya existente sobre protección de datos personales y adaptarla al nuevo contexto mundial que después del caso de *Cambridge Analytica* cambio notablemente. Con el GDPR la UE estableció todo un sistema de protección de datos personales, que modifico reglas ya existentes, desarrolló aquellas que eran muy básicas y creó otras que eran necesarias. Además, siendo de obligatorio cumplimiento y aplicación directa en los Estados pertenecientes a la UE no requiere transposición, lo que acelera la eficacia de la aplicación de la norma en los Estados (Ortega y Domenech, 2018, p. 4). Esta novedad se orienta a una transición hacia una economía centralizada en los datos y la creación de un mercado único digital (Moritz y Gibello, 2017, p. 116).

Respecto a la TIDP con el GDPR en la UE se estableció un conjunto de mecanismos para transferir datos a terceros países: decisiones de adecuación, normas contractuales estándar, normas corporativas vinculantes, mecanismos de certificación y códigos de conducta. En la UE con el GDPR para realizar una

TIDP se requiere un nivel adecuado de protección. Razón por la que Estados Unidos debió implementar el *Privacy Shield*, y Latinoamérica se encuentra en proceso de adopción y aplicación de estándares internacionales para la protección de datos personales.

En el GDPR existen 3 niveles de protección a efectos de autorizar una TIDP a un tercer país u organización internacional. La regla general es cumplir con un nivel adecuado de protección, que es el nivel más riguroso, después viene el nivel de ofrecer garantías adecuadas; y el establecimiento de normas corporativas vinculantes o certificaciones. Además, existen casos excepcionales para realizar una TIDP. De tal manera para analizar exhaustivamente este tema en la siguiente tabla de explicará 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 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.	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.

	Además, los interesados cuenten con derechos exigibles y acciones legales efectivas. Con autorización de autoridad de control: **a)** Cláusulas contractuales. **b)** Acuerdos administrativos.	**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 autoridad de control competente.	Deben ser jurídicamente vinculantes, aplicarse y ser cumplidas por. Además, deben conferir expresamente derechos a los interesados. Además, las normas corporativas como mínimo deben especificar, los elementos que señalados para la TIDP mediante garantías adecuadas.

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

Adicionalmente, en caso de que no se puedan cumplir con alguno de estos niveles de protección una TIDP puede realizarse en los siguientes casos conforme el Art 49 del GDPR:

a) Consentimiento explícito del interesado.
b) La TIDP sea necesaria para la ejecución de un contrato entre el interesado y el responsable del TDP.
c) La TIDP sea necesaria para le ejecución de medidas precontractuales adoptadas a solicitud del interesado.
d) La TIDP sea necesaria para la celebración o ejecución de un contrato, en interés del interesado.
e) La TIDP sea necesaria por razones importantes de interés público.
f) La TIDP sea necesaria para la formulación, el ejercicio o defensa de reclamaciones.
g) La TIDP sea necesaria para proteger los intereses vitales del interesado.
h) La TIDP se realice desde un Registro Público con arreglo al Derecho de la UE.
i) También puede realizarse una TIDP en el caso de que esta no sea repetitiva, afecte solo a un número limitado de interesados, sea

necesarias 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.

Conforme lo anterior, estos 3 niveles y casos excepcionales son el estándar europeo de protección para realizar una TIDP, el cual se diferencia bastante del americano que sólo cuenta con normas corporativas vinculantes para la TIDP. Estos criterios se usarán el capítulo siguiente para determinar el estándar de protección que requiere el Ecuador. Siguiendo con el objeto de la investigación en la siguiente tabla se realizará una comparación entre la Directiva 95/46/CE y el GDPR respecto a la TIDP y 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: cambios sustanciales entre la Directiva 95/46/CE y el GDPR respecto a la TIDP.

2.3 Referentes de América Latina en la regulación de la protección de datos personales

En América Latina la regulación del derecho a la protección de datos personales sigue un ritmo propio y tiene ciertas características que ameritan analizarse. Recientemente en las constituciones latinoamericanas se incorporó como derecho autónomo a la protección de datos personales frente a la necesidad de dar respuesta al proceso de evolución tecnológica (Ordóñez, 2017, p. 85). En los países latinoamericanos la protección de datos personales derivó de la necesidad de proteger los derechos fundamentales de las personas que pueden ser afectados por el TDP (Remolina et al., 2018, p. 68).

Por esta razón, y para seguir el objeto de la presente investigación se efectuará una comparación de las legislaciones sobre datos personales de 3 países (Argentina, México y Brasil), para luego compararlo con los modelos de protección de datos personales americano y europeo. Poniendo énfasis, en el desarrollo de esta legislación y como se ha seguido las tendencias regulatorias mundiales sobre este tema en Latinoamérica.

2.3.1 República de Argentina

En el Art. 43 de la Constitución de la República de Argentina se encuentra consagrado el derecho a la protección de datos personales. En este artículo se deriva la obligación de los organismos públicos de garantizar el acceso a la información, confidencialidad, supresión y rectificación de los datos personales. Pero, es en la Ley 25.336 promulgada el 4 de octubre del año 2000 donde se encuentra reglamentada la protección de datos personales. En el Art. 2 de la mencionada Ley se regula la protección de datos personales sin hacer una 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. Destacándose, el principio de licitud para la formación de archivos de datos. El principio de calidad de datos que se traduce en que la recolección de datos no puede hacerse por medios desleales y que dichos datos deben ser ciertos y exactos, y su almacenamiento debe permitir el derecho de acceso a su titular. El principio de la información en el sentido de que se debe informar a los titulares para qué serán tratados los datos y quiénes serán sus destinatarios y el principio de responsabilidad demostrada.

En Argentina conforme el Art. 29 el órgano de control que gozara de autonomía funcional y actuara como órgano descentralizado en el ámbito del ministerio de justicia y Derechos Humanos de la Nación es la Agencia de Acceso a la Información Pública, la cual es la encargada de supervisar que se cumplan las disposiciones contenidas en la Ley 25.326, en la Ley de Acceso a la Información, y en la Ley del Registro No Llame. Respecto a la TIDP se sigue el modelo europeo toda vez que en el Art. 12 se exige para autorizar una TIDP que el Estado receptor de los datos cuente con un nivel adecuado de protección.

2.3.2 Estados Unidos Mexicanos

El caso mexicano es particular, recién con las reformas constitucionales del año 2007 y 2009 es que se protege constitucionalmente a los datos personales, se consagra explícitamente el derecho a la protección de los datos personales y se establecen los derechos ARCO como núcleo fundamental de dicho derecho (Da Cunha, 2011, p.323). Posteriormente, en el año 2010 se adopta la Ley Federal de Protección de Datos en Posesión de Particulares, teniendo un ámbito de aplicación únicamente privado. Dada la redacción de esta Ley es evidente que se basa en el marco normativo europeo apuntando 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 establece las competencias de la Autoridad reguladora, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). En el capítulo IV en relación con el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de 21 diciembre 2011, regula los derechos ARCO. En capítulo V se desarrolla la TIDP, pero, no se exige un nivel adecuado de protección, tan solo exige consentimiento del titular de los datos y enumera ciertos supuestos que no requieren consentimiento, además no desarrolla las transferencias ulteriores.

El 26 de enero de 2017, se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados con el fin de regular el ámbito público del TDP. Son sujetos obligados conforme el Art. 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 le son aplicables 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 se desarrolla un conjunto de principios que el responsable del tratamiento debe cumplir cuando recolecta, almacena, usa, circula o realiza cualquier actividad con datos personales, como son los: principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad demostrada en el TDP. De la autoridad de protección de datos personales señala que sigue siendo el INAI. En lo que se refiere a la TIDP en el Art. 68 de la Ley aplicable a los sujetos obligados se señala 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.”

De esta norma se evidencia que para autorizar una TIDP se exige el cumplimiento de garantías adecuadas, además de necesitar el responsable del TDP 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.

2.3.3 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 otorgarle protección, conforme el Art. 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 el año 2018 promulgó una interesante ley de protección de datos que entrará en vigor en el año 2020 que regula tanto el ámbito privado como público, muy parecida al GDPR de la UE.

En relación a la TIDP el Art. 33 de la Ley General de Protección de Datos brasileña (LGPD) indica que la TIDP sólo 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 ofrece 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 no. 869/18 por la que se creaba la Autoridad Nacional Brasileña de Protección de Datos. La medida vino a complementar la LGPD y 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.

2.3.4 Estándares de protección de datos personales para los Estados Iberoamericanos (2017)

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, donde se alcanzó un acuerdo con la asistencia de representantes de 14 países iberoamericanos. Desde el 2003 La RIPD se configura como un foro que integra varios actores, tanto del sector público como 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 adoptados en el año 2017, aplicables 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 principios, derechos, sanciones y TIDP con ciertas particularidades acorde a las necesidades de los países iberoamericanos. De tal

modo, constituyen una serie de directrices para la emisión de normativas regulatorias de protección de datos personales en la región iberoamericana y sirvan de ser el caso como referente para la modernización y actualización de las legislaciones existentes.

Tabla 9.

Comparación entre la 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: comparación entre las normativas de protección de datos de países latinoamericanos y los estándares de la RIPD. El símbolo “- “significa que no aplica.

2.4 Organizaciones internacionales que regulan los flujos transfronterizos de datos personales

2.4.1 La Organización para la Cooperación y el Desarrollo Económicos (OCDE)

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 fundamentándose 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 privacidad de la OCDE definen conceptos fundamentales en materia de protección de datos, permiten una común aplicación a los sectores

público y privada y garantizan el libre flujo de datos personales sujeto al respeto a 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 serían más tarde los principios básicos en la protección de datos (Saltor, 2013, p. 107).

Estas directrices exigen un estándar mínimo de protección para el flujo transfronterizo de datos personales, sin embargo, autoriza la restricción del flujo cuando un país no provee un nivel de protección equivalente (Portas, 2012, p.417) Cabe indicar, que para este nivel equivalente de protección de datos la presencia de una autoridad de control independiente es condición necesaria para cumplir con dicho estándar (Cerda, 2011, p. 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 garantice a los titulares de los datos el respeto a sus derechos fundamentales cuando sus datos son objeto de una TIDP.

En el año 2013 la OCDE adopta su *Privacy framework,* documento mediante el cual se actualizó las directrices sobre privacidad de 1980, realizando 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 afecten los datos personales. Adicionalmente, Remolina (2018, p.) indica que se introdujo el concepto de los programas de gestión de privacidad que son el mecanismo operativo, medio por el que las organizaciones implantan la protección de privacidad y de los datos personales.

2.4.2 Foro de Cooperación Económica Asia-Pacífico (APEC)

En 2004 se expidió el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico o APEC *Privacy Framework*. En el documento, se estableció marco para la regulación del tratamiento de la información personal adoptado por las economías que integran el APEC, mediante el cual se procura el establecimiento de un estándar de protección que no implique trabas para el comercio internacional entre los países miembros. Es un programa de 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 de principios generales que guíen la regulación interna de las economías de Asia, en relación 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 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.

2.5 Comparación entre las regulaciones sobre la TIDP

Del estudio realizado se evidenció que el derecho a la protección de datos personales se tutela de una manera diferente a nivel mundial, aunque con una tendencia a dirigirse al modelo europeo. Además, debido a los riesgos de la TIDP, desde 1980 con las directrices sobre privacidad de la OCDE se ha marcado una predisposición de los Estados y las organizaciones internacionales de exigir un nivel adecuado de protección de datos personales para autorizar una TIDP. Así pues, a partir del análisis realizado sobre la regulación de la protección de datos personales, corresponde efectuar una comparación centrada en los temas que son objeto de la presente investigación, con el fin de

delimitar elementos comunes para identificar el estándar adecuado de protección de datos personales para la TIDP aplicable al Ecuador.

Tabla 10.

Comparación con respecto a la protección de datos personales

	América Latina			Europa		Organismos Internacionales	
	Argentina	**México**	**Brasil**	**GDPR**	**EE.UU.**	**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: 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**	***Privacy Shield***	**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: 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, las legislaciones latinoamericanas y los organismos internacionales se alinean al estándar de protección de datos personales que establece la UE con el GDPR. Se resalta la necesidad de contar con autoridades de control autónomas como la AEPD en España o la CNIL en Francia para un correcto desarrollo de la protección de datos. En cuanto a la TIDP de igual manera se sigue la tendencia europea de establecer niveles de protección adecuados que permitan proteger a los titulares de los datos. Además, los parámetros para verificar que un Estado cuente con un nivel de protección adecuada a fin de autorizar una TIDP son los que establecía la Directiva 95/46/CE y ahora el GDPR (Bu-Pasha, 2017, p. 219).

En resumen, la regulación de TIDP intenta equiparar dos intereses jurídicos sin que ninguno se vea perjudicado, por una parte, no impedir los flujos transfronterizos de datos personales, necesarios para el comercio internacional y, por otra parte, la protección de las personas en lo que a sus datos personales. Por consiguiente, para cumplir con el objetivo de esta investigación, a continuación, se realizará una explicación y estudio de la situación actual del Ecuador en cuanto a la protección de datos personales y la TIDP, para poder con los parámetros obtenidos en este y el capítulo anterior determinar en qué situación se encuentra el Ecuador y hacia donde debe orientarse en esta materia.

3 CAPÍTULO III. ESTÁNDAR ADECUADO DE PROTECCIÓN PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES EN EL ECUADOR

Desde la incorporación y posterior desarrollo de las nuevas tecnologías (Internet) el Ecuador ha pasado por una revolución en el manejo de la información. La combinación de estas herramientas tecnológicas con el fenómeno de la globalización trajo consigo múltiples ventajas, por ejemplo: 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, p. 54). Todas estas

actividades requieren de un TDP o de una TIDP. De tal manera, son varios los países que regulan la protección de datos personales para proteger los derechos de sus ciudadanos, fomentar el desarrollo de empresas de servicios cuyo objeto de negocios es la información y desarrollar el comercio internacional y electrónico que dependen de una correcta regulación de la TIDP.

El Ecuador en este contexto, no cuenta con una regulación que garantice un nivel adecuado de protección de datos personales. Lo cual, se evidencia porque la protección de datos personales en el país es incompleta, sectorial, contradictoria y desactualizada. Por lo que, es insuficiente para proteger adecuadamente los derechos de los titulares de datos personales y, además, es inexistente respecto a la TIDP. Por esta razón, a partir de un recuento y análisis de la normativa que regula la protección de datos en el Ecuador y con las bases obtenidas de los capítulos previos de la presente investigación, se comprobarán estas aseveraciones. Para luego, continuar con el objeto de la presente investigación que es determinar cuál estándar de protección se debe cumplir para contar con un nivel adecuado de protección para la TIDP en el Ecuador.

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

3.1 Situación actual de la protección de datos personales en el Ecuador

En el Ecuador se han presentado dos proyectos de ley para regular la protección de datos personales, el primero en el año 2010 por el asambleísta Vethowen Chica y el segundo en el año 2016 por la asambleísta Gabriela Rivadeneira. El primer proyecto fue archivado por sus amplias falencias, mientras que el segundo desde el año 2016 no se le ha dado continuación. No obstante, desde el año 2017 la Dirección Nacional de Registros de Datos Públicos (DINARDAP) ha realizado una ardua labor para redactar un nuevo proyecto de ley que cumpla con estándares internacionales y pueda ser aplicada a la realidad ecuatoriana. Esta propuesta ha sido socializada con expertos y con la comunidad en general.

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

Tabla 12.

Desarrollo normativo de la protección de datos personales en el 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 a 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. 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 datos personales sensibles.
Código Orgánico Integral Penal (2014)	**Art. 12:** Derecho de protección a los datos personales de loa 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 dato 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 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: normativa ecuatoriana que regula la protección de datos personales hasta la actualidad. Un análisis detallado se encuentra en el Anexo 1 de la presente investigación.

Si bien la Constitución del Ecuador reconoce el derecho a la protección de datos personales, la normativa interna, aunque regula en varios cuerpos normativos este derecho no lo hace correctamente, es insuficiente para otorgar una adecuada protección a los titulares de los datos personales. Conforme el análisis del ordenamiento jurídico ecuatoriano se evidencio que regula esta materia de forma sectorial, lo cual estaría bien si es que lo hiciera de forma completa, sin embargo, la regulación al estar desperdigada en varios cuerpos normativos es incompleta y en muchos casos contradictoria. Existen algunos parámetros para el TDP de datos públicos, pero no se desarrolla todos los principios necesarios para un adecuado TDP, 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 cuenta con una autoridad de control y respecto al TDP en el ámbito privado y sobre la TIDP no existe regulación.

En relación con lo anterior, la normativa también se encuentra esta desactualizada y en muchos casos es errónea, ya que los conceptos o están mal desarrollados, o ya no responden a los avances tecnológicos, como los conceptos de ficheros o de dato personal. Sus leyes no permiten ejercer adecuadamente del derecho a la protección de datos personales. Por esta razón,

con el fin de reafirmar la afirmación de que la protección de datos en el Ecuador es insuficiente, en la siguiente tabla se realizará una comparación del Ecuador con otros países de la región, respecto a los elementos fundamentales que debe ofrecer un sistema de protección de datos personales para proteger los derechos de sus ciudadanos.

Tabla 13.

Comparación entre Ecuador y otros países latinoamericanos respecto a la protección de datos personales

	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	✓	✓	✓

Nota: análisis de la regulación sobre protección de datos personales de otros países de la región con respecto a Ecuador. *Por el Hábeas Data se ejercen los derechos ARCO, pero tal como está concebido en la normativa ecuatoriana no permite ejercer todos, como el de limitación al TDP.

El Ecuador en comparación con otros países de la región no cuenta ni con un nivel mínimo de protección de datos personales. Los tres países con los que se realizó la comparación conforme los capítulos previos de la presente investigación se orientan al modelo europeo de protección de datos, por lo cual el Ecuador tampoco cumplirá con los niveles de protección que exige la UE. Con esto queda en evidencia que la regulación con la que cuenta Ecuador para la protección de datos personales no sólo es insuficiente, no brinda garantías adecuadas a los titulares de los datos personales. En relación con el tema de la presente investigación, tomando en cuenta que la regulación respecto a la TIDP

en el Ecuador es inexistente, prosigue analizar las propuestas de ley antes mencionadas para verificar si alguna de ellas cumple algunos de los elementos necesarios para contar con un nivel adecuado de protección para la TIDP.

3.2 Propuestas de ley presentadas en el Ecuador para regular la protección de datos personales

En el Ecuador se han presentado dos proyectos de ley respecto a la protección de datos personales. Específicamente de estos proyectos se analizará de forma general la protección de datos personales que brinda y las normas pertinentes a la TIDP con el fin de evaluar si estos cumplen con los estándares de protección analizados en la presente investigación. Respecto al anteproyecto de ley de la DINARDAP se analizará si puede acercar al país a cumplir con un nivel adecuado de protección para que le permita realizar TIDP con un tercer país u organización internacional.

a) Proyecto de Ley de Protección a la Intimidad y a los Datos Personales (2010)

Fue presentado por el asambleísta Vethowen Chica, el 16 de marzo del año 2010, fue objeto de dos debates en los cuales se realizaron varias observaciones que resultaron en 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, creación de un organismo administrativo denominado “Dirección Nacional de Protección de Datos Personales” que en si no sería una autoridad de control autónoma, 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 se encontraban ambiguos y no se contemplaba un capítulo para regular la TIDP ni las sanciones por la violación de esta ley.

b) Proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales (2016)

El proyecto fue presentado por la asambleísta Gabriela Rivadeneira el doce de julio del año 2016. El primer debate se realizó el día 5 de octubre del año 2016, en el cual se recalcó que la pretensión de este proyecto es proteger los datos personales tanto en el ámbito público como privado puesto que un mal uso de los datos personales pone en riesgo 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 de ley presentó varias falencias, comenzado desde su objeto donde señala a la intimidad, luego en conceptos básicos como: dato personal, responsable del tratamiento de la información, usa la palabra información en vez de dato personal, encargado del TDP lo confunde con responsable del archivo, registro, base o banco de datos. No desarrolla correctamente los principios rectores de la protección de datos y deja de lado el de responsabilidad, licitud y seguridad. Pretende conforme el Art. 16 que todas las bases o bancos de datos, ficheros o archivos tanto de públicos como de privados con fines exclusivamente financieros y mercantiles deberán inscribirse en el Registro Nacional de Bases de Datos Personales vulnerando todo el sentido de la protección de datos personales al ser el Estado, él que pueda tener acceso a todos los datos personales (Enríquez, 2017, p. 56).

En cuanto a la TIDP ni desarrolla como se evaluará si un tercer país u organización internacional cuenta con un nivel de protección adecuado, ni da la posibilidad de utilizar normas corporativas vinculantes para realizar un TIDP. Señala como Autoridad Nacional de Protección de Datos Personales 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 si la DINADARP es realmente el órgano adecuado para proteger y ejercer la tutela de los datos personales ya que, si no se cuenta con un organismo de control que cumpla con los estándares mínimos para la protección de datos, el Ecuador para el resto del mundo seguirá sin contar con un nivel adecuado de protección de datos personales.

c) Anteproyecto de la Ley Orgánica de Protección de datos Personales (2019)

La formación del anteproyecto de ley de la DINARDAP se realizó desde el año 2017, el cual a diferencia de los dos proyectos de ley anteriores tuvo la participación de la sociedad civil, la academia, abogados especializados en protección de datos personales, técnicos expertos en seguridad de la información y con 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 quien juega un doble rol, el de garante del derecho a la protección de datos y como responsable del tratamiento de ciertos datos. Los objetivos de este anteproyecto 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.

Para realizar el análisis de este anteproyecto se ha tomado el último borrador puesto a disposición del público el 28 de mayo del año 2019. Este borrador se encuentra estructurado en 10 capítulos, que recogen las tendencias internacionales respecto a la regulación de la protección de datos personales. En el primer capítulo se establece disposiciones directivas respecto al objeto, finalidad, ámbito de aplicación material, territorial del anteproyecto, y 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, aquí se nota la influencia de otras leyes en la materia como la mexicana y española. No obstante, entre los principios que se destacan, se encuentran el de responsabilidad proactiva y demostrada tomada de las Directrices sobre Privacidad de la OCDE y adoptada por el GDPR.

En el tercer capítulo se desarrolla los derechos de los titulares de los datos, los cuales siguen la tendencia europea de a más de los derechos ARCO aumentar el de portabilidad. En el cuarto capítulo se establece un régimen especial para el TDP de datos sensibles. El quinto capítulo desarrolla las medidas de seguridad

que deben tomar los responsables o encargados del TDP, adopta la figura del delegado de protección de datos personales, la de los códigos de conducta y los mecanismos de certificación. En el sexto capítulo desarrolla la TIDP, el cual tiene una muy fuerte influencia del GDPR adopta prácticamente su regulación respecto a este tema y los niveles por los cuales se realiza una TIDP en la UE.

En el capítulo séptimo se establecen las obligaciones a los responsables o encargados del TDP. En el octavo capítulo se regula las reclamaciones directas que puede realizar el titular de los datos personales al responsable del TDP. En el noveno capítulo se establece un régimen sancionatorio pecuniario con ciertas medidas provisionales o cautelares. Por último, en el décimo capítulo se trata sobre la autoridad de control y se pretende que sea la DINARDAP. En las disposiciones generales, transitorias, derogatorias se busca una adaptación a las demás normas ecuatorianas. En general, esta propuesta de regulación a diferencia de los otros proyectos de ley que se analizado mejora bastante. Sin embargo, se puede notar todavía ciertos errores que podrían causar varios inconvenientes al momento de su aplicación, como la autoridad de control.

El anteproyecto tiene la influencia de normativas sobre datos personales, como el GDPR, la ley uruguaya, mexicana y española, por lo que cuenta con los cambios regulatorios que se han dado a nivel internacional. Sin embargo, aún le falta corregir errores, incluir algunas disposiciones y desarrollar más ciertas figuras para lograr regular adecuadamente la protección de datos personales. No obstante, es una muy buena iniciativa de la DINARDAP para que el Ecuador promueva la TIDP y proteja a los titulares de los datos personales. Con el fin de evidenciar los problemas de las propuestas de ley analizadas previamente, en la siguiente tabla se realiza una comparación poniendo énfasis en la TIDP.

Tabla 14.

Comparación entre las propuestas de ley que se han presentado en el Ecuador respecto a la protección de datos personales y la TIDP

	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	✓
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	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: análisis especifico de los temas referentes a la TIDP.

Los proyectos de ley no llegan a cumplir con un nivel suficiente de protección de datos personales y menos aún regulan adecuadamente la TIDP. En cuanto al anteproyecto, mejora notablemente respecto de las dos propuestas anteriores, en general para regular el TDP cumple con los elementos mínimos necesarios. Sin embargo, hay cuestiones como la definición de dato personal, la cual a diferencia de otras legislaciones es bastante complicada, lo que puede producir confusión y tergiversación al momento de determinar que es un dato personal.

En cuanto a la TIDP no ofrece una definición y no desarrolla adecuadamente las TIDP ulteriores, pero establece 3 niveles de protección para realizar una TIDP y casos excepcionales para la TIDP, lo cual será posteriormente analizado. Respecto al tema de las sanciones es peculiar, ya que para establecer una sanción pecuniaria son muy elevadas los porcentajes y se utiliza el término

volumen del negocio, lo cual produce confusión y no se tiene claridad de como calcular la sanción. Lo más preocupante es la autoridad de control, ya que la DINARDAP es un órgano que forma parte de la función ejecutiva. Cabe entonces la duda de si la DINARDAP 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.

3.3 Niveles de protección adecuados para realizar una TIDP

En la presente investigación se ha evidenciado que la regulación actual sobre protección de datos en el Ecuador es insuficiente y en cuanto a la TIDP es inexistente. A partir del análisis de los dos 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 Ecuador. Los dos proyectos no cumplen con los estándares de protección que se ha estudiado en los capítulos previos.

No obstante, el análisis del anteproyecto de ley arrojó, que si bien cuenta con ciertas falencias pretende regular la protección de datos personales de una forma mucho mejor que la actual y que la que ofrecían los dos proyectos. Además, respecto a la TIDP presenta aspectos que requieren su análisis. Por estas razones, en esta parte de la investigación, a partir de los estándares de protección para la TIDP estudiados en los capítulos previos, se mostrará el nivel en el que se encuentra el Ecuador y en cual se encontraría si se llegará a promulgar el anteproyecto de ley de la DINARDAP. El estándar europeo es el que se tomara para realizar el análisis dado que es el más seguro, el cual consta de tres niveles y un conjunto de excepciones para realizar un TIDP.

El primero es contar con una Decisión de autoridad de control competente de que ese Estado garantiza un nivel de protección adecuado, este nivel es el más exigente. El Ecuador conforme a lo que se analizado en la presente investigación 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 legislación pertinente en la materia, no tiene una autoridad de control independiente, ni adoptado ninguna normativa internacional respecto a la protección de datos.

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

El tercer nivel es realizar una TIDP mediante normas corporativas vinculantes, que como el caso anterior el Ecuador al no regular nada sobre la TIDP y las normas corporativas, y tampoco ofrecer una protección adecuada con su normativa no podría realizar TIDP por medio de estas normas. El último medio por el cual el 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, porque son necesarias por interés público o para proteger los intereses vitales del titular de los datos.

No obstante, la situación variaría en el Ecuador si es que se aprueba el anteproyecto de ley de protección de datos personales de la DINARDAP, ya que al ser analizado se mostró que regula de una mejor manera la protección de datos personales, por lo cual pudiera realizar TIDP por cualquiera de los medios antes señalados. Sin embargo, el primer nivel que es contar con un nivel adecuado de protección declarado por una autoridad de control competente se pone en duda ya que en el anteproyecto se establece a la DINARDAP como

organismo de control y como ya se señaló este no es independiente, por lo que tendría que cambiar eta autoridad para lograr este nivel adecuado. Para evidenciar estas afirmaciones en la siguiente tabla se muestra como el Ecuador realiza TIDP y como con la aprobación del anteproyecto las podría realizar.

Tabla 15.

Comparación entre los niveles de protección para la TIDP

País o Unión de países	**Niveles de protección de datos personales con los que cuentan para realizar un TIDP**	**Nivel con el que puede realizar una TIDP con el Ecuador**	
		Actual	**Con el Anteproyecto**
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 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.

Nota: análisis de la situación actual del Ecuador respecto a la protección de datos y como se vería con la aprobación del anteproyecto de ley.

3.4 Estándar de protección adecuado para realizar TIDP en el Ecuador

Tomando en cuenta que con la actual normativa el Ecuador para la TIDP se encuentra en los casos excepcionales, se requiere adoptar una ley de protección de datos personales que permita realizar una TIDP de maneras más seguras. Por ende, la aprobación del anteproyecto de ley llevaría al Ecuador a contar con

un nivel para realizar TIDP más alto y seguro, es necesario determinar si los niveles de protección que establece el anteproyecto de ley para permitir estas transferencias responden al estándar de protección adecuado que requiere el Ecuador. Así pues, 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.

Niveles adecuados de protección para la TIDP y sus beneficios económicos

Niveles para realizar una TIDP	Países con los que se puede realizar un TIDP por este nivel	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 constituye para el Ecuador uno de sus principales socios comerciales con exportaciones de más de 2.000 millones de USD y ahora aún más por el acuerdo comerciales 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, Philipinas, Corea del Sur	El 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 que se regule 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, reflejan que las exportaciones a Estados Unidos sumaron $ 2.536 millones en el 2018. Estas cifras demuestran que este país es el principal socio comercial del 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 pudiera crear nuevas oportunidades de negocios. De igual forma, la TIDP con países latinoamericanos, debe ser prioridad del Ecuador para fortalecer lazos y relaciones comerciales.

Adaptado de (Fedexport, 2019, pp. 1-6).

Nota: análisis de los niveles adecuados de protección para la TIDP y los beneficios económicos que traería regular en el anteproyecto de ley estos niveles.

A partir de este análisis se evidencia que el estándar de protección adecuado para la TIDP que debe adoptar el Ecuador debe regular los 3 niveles de protección para realizar una TIDP y los casos excepcionales. Lo cual, servirá para desarrollar el comercio internacional y electrónico con sus principales socios comerciales. Este estándar es el europeo, que como se demostró es el que siguen los demás países latinoamericanos, los organismos internacionales y hasta Estados Unidos con la CCPA.

Por esta razón, el anteproyecto presentado por la DINARDAP estaría regulando adecuadamente la TIDP, ya que toma en cuenta la mayoría de estos parámetros a efectos de permitir una de estas transferencias, permitiendo 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 tema de la autoridad de control, el concepto de dato personal, incluir un concepto de TIDP, desarrollar las TIDP ulteriores y arreglar el régimen sancionatorio para que el Ecuador pueda conseguir contar con un nivel adecuado de protección.

Entonces, si el Ecuador si quiere favorecerse completamente de los intercambios comerciales con Europa, 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 y particularmente en Europa. Así lo señala Grande (2016, p. 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.”.

4 CONCLUSIONES

De la investigación realizada se extraen las siguientes conclusiones:

A nivel internacional por los riesgos que implica una TIDP se ha buscado una armonización de criterios en cuanto a su regulación, de modo que se pueda establecer un nivel mínimo de protección con el que deben contar los países para poder efectuar una TIDP. La UE y Estados Unidos son quienes más han desarrollado este tema, por lo que sus modelos de protección de datos personales son los que a nivel mundial tienen mayor relevancia. No obstante, tienen enfoques distintos, Estados Unidos adopta un enfoque sectorial y de autorregulación, mientras que la UE adopta un enfoque fundamentado en una norma general de aplicación extraterritorial, 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. Motivo por el que los varios países y organismos internacionales, como Brasil, México, la APEC y la OCDE se encuentran siguiendo el estándar europeo de protección de datos. El caso de Estados Unidos es particular, ya que, si bien regula la protección de datos, no lo hace adecuadamente. No obstante, dado 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 cumple con los elementos y parámetros que exige el GDPR para permitir una TIDP, por lo que tarde o temprano se invalidará este acuerdo. Para contrarrestar esto, en Estados Unidos, específicamente en el Estado de California por su tradición tecnológica se implementará en el año 2020 el CCPA, normativa que sigue la tendencia europea en cuanto a la protección de datos personales.

A la luz de las constataciones anteriormente expuestas, para garantizar un nivel adecuado de protección para la TIDP el Ecuador debe adoptar el estándar europeo de protección. El cual, consiste en establecer 3 niveles de protección y

una serie de casos excepcionales. Los niveles de protección como se mostró en los capítulos previos exigen el cumplimiento de una serie de principios, mecanismos, normas y compromisos que deben cumplir los Estados a efectos de que se autorice 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 sustancialmente equivalente al brindado por el GDPR.

Como se pudo demostrar la regulación sobre protección de datos personales en el Ecuador es ineficiente, dado que se encuentra dispersa, incompleta, desactualizada y es contradictoria. Además, en base al 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 el 2010 y otro en el 2016, los cuales conforme el análisis realizado en esta investigación se demostró que tienen varias deficiencias. No obstante, en la actualidad existe un anteproyecto de ley creado por la DINARDAP, el cual presenta notables mejoras en la regulación de esta materia, sin embargo, requiere arreglar ciertos problemas para poder constituirse en una normativa que pueda asegurar un adecuado nivel de protección de datos personales a la luz del estándar europeo.

El anteproyecto de ley de la DINARDAP sirvió en la presente investigación, como referencia de lo que el Ecuador debe realizar en materia de protección de datos personales. Respecto a la TIDP, establece 3 niveles de protección y casos excepcionales siguiendo el estándar de protección europeo. Por esta razón, acerca al Ecuador a contar con un nivel adecuado de protección de datos. Lo cual mediante el análisis de los beneficios que obtendría el Ecuador siguiendo este estándar, se evidenció que debe adoptarlo para poder realizar TIDP con sus principales socios comerciales, como Estados Unidos, la UE, China, Rusia y con Latinoamérica, y, por ende, mejorar la competitividad de las empresas ecuatorianas e impulsar, promocionar y desarrollar el comercio internacional.

La promulgación en el Ecuador de una ley de protección de datos personales permitirá regular la forma en que las empresas nacionales y extranjeras, además

de los entes públicos utilizan, procesan, conservan y explotan los datos personales de las personas naturales en el Ecuador. El anteproyecto de la DINARDAP es la mejor opción con la que cuenta el país respecto a este tema, dado que su aprobación traería la oportunidad tanto de desarrollar el comercio internacional, como de proteger los datos personales de sus ciudadanos. Ahora bien, se recomienda la inclusión de ciertas precisiones en el anteproyecto, como: definir una autoridad de control independiente, acortar y mejorar el concepto de dato personal, incluir los conceptos de TIDP, exportador e importador de datos, desarrollar las TIDP ulteriores y definir otra forma de cálculo para aplicar las sanciones pecuniarias y disminuir los porcentajes del cálculo de estas sanciones.

REFERENCIAS

Alexy, R. (1993). *Teoría de los derechos fundamentales.* Madrid: Centro de Estudios Constitucionales.

Asamblea Nacional del Ecuador. (s.f.). *Proyecto de Ley de Protección a la Intimidad y a los Datos Personales de 2010*. Recuperado el 28 de mayo de 2019 de http://ppless.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/1f0a354a-3380-46d8-b828-f912f5dc13cf/Proyecto%20de%20Ley%20de%20Protecci%C3%B3n%20a%20la%20Intimidad%20y%20a%20los%20Datos%20Personales%20Tr.%2025508.pdf

Asamblea Nacional del Ecuador. (s.f.). *Proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales de 2016.* Recuperado el 28 de mayo de 2019 de 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

Bryan Cave Leighton Paisner LLP. (2018). *California Consumer Privacy Act (CCPA). Practical Guide.* Recuperado el 14 de abril de 2019 de https://www.bclplaw.com/images/content/1/5/v2/159052/BCLPs-Practical-guide-to-the-CCPA-USA01-12167951.pdf

Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law, 26*(3). Recuperado el 25 de abril de 2019 de

https://www.tandfonline.com/doi/pdf/10.1080/13600834.2017.1330740?needAccess=true

Castellanos Rodríguez, A. (2017). El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio Privacy Shield. *ICPS Working Papers*, 350. Recuperado el 15 de mayo de 2019 de https://www.icps.cat/archivos/Workingpapers/wp350.pdf?noga=1

Cerda, A. (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. Recuperado el 17 de mayo de 2019 de https://scielo.conicyt.cl/pdf/rdpucv/n36/a09.pdf

Cobb, S. (2019). GDPR: ¿el primer paso hacia una ley de privacidad global? *ESET*. Recuperado el 20 de mayo de 2019 de https://empresas.eset-la.com/archivos/novedades/74/Cybersecurity_Trends_2019_v6-ESP.pdf

Código de la Niñez y Adolescencia. (2003). Registro Oficial 737, Suplemento, de 03 de enero de 2003. Última modificación: 06 de mayo de 2019.

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

Código Orgánico General de Procesos. (2015). Registro Oficial 506, Suplemento, de 22 de mayo de 2015. Última modificación: 21 de agosto de 2018.

Código Orgánico Integral Penal. (2014). Registro Oficial 180, Suplemento, de 10

de febrero de 2014. Última modificación: 03 de junio de 2019.

Código Orgánico Monetario y Financiero Libro I. (2014). Registro Oficial 332, Suplemento, de 12 de septiembre de 2014. Última modificación: 19 de marzo de 2019.

Comisión Europea. (s.f.). *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*. Recuperado el 4 de mayo de 2019 de 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.* Recuperado el 18 de mayo de 2019 de https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062

Constitución de la República del Ecuador. (2008). Registro Oficial 449 de 20 de octubre de 2008. Reformas: Registro Oficial 490, Suplemento, de 13 de julio de 2011 y Registro Oficial 653, Primer Suplemento, de 21 de diciembre de 2015. Última modificación: 30 de abril de 2019.

Constitución Política de la República del Ecuador. (1998). Registro Oficial 1 de 11 de agosto de 1998. Última modificación: 20 de octubre de 2008. Estado: derogado.

Corte Constitucional de Colombia. (s.f.). *Sentencia C-748/11 de la Corte Constitucional de Colombia de 6 de octubre de 2011.* Recuperado el 16 de abril de 2019 de http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

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

Corte Europea de Derechos Humanos. (s.f.). *Caso Amann vs. Suiza sentencia de 16 de febrero de 2000, asunto 27798/95 del Tribunal Europeo de Derechos Humanos 2000-II.* Recuperado el 30 de marzo de 2019 de https://hudoc.echr.coe.int/spa#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-162541%22]}

Corte Europea de Derechos Humanos. (s.f.). *Caso Leander vs. Suecia sentencia de 26 de marzo de 1987, asunto 9238/81 del Tribunal Europeo de Derechos Humanos, Corte Chamber.* Recuperado el 17 de mayo de 2019 de https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}

Corte Europea de Derechos Humanos. (s.f.). *Caso Z vs. Finlandia, sentencia de 25 de febrero de 1997, asunto 9/1996/627/811 del Tribunal Europeo de Derechos Humanos.* Recuperado el 15 de abril de 2019 de https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58033%22]}

Cunha, T. D. (2011). Las recientes reformas en materia de protección de datos personales en México. *Anuario Jurídico y Económico Escurialense*. Recuperado el 29 de marzo de 2019 de https://webcache.googleusercontent.com/search?q=cache:QvlznE2PZ80J:https://dialnet.unirioja.es/descarga/articulo/3625376.pdf+&cd=1&hl=es&ct=clnk&gl=ec

Davara Rodríguez, M. (2006). *Manual de Derecho Informático.* Madrid: Thompson Aranzadi.

Davara, I. (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, M. (2011). La institucionalización de la protección de datos de carácter personal. En R. Arrieta, Reflexiones Sobre el Uso y Abuso de los Datos Personales en Chile (pp. 55-79). Santiago de Chile: Expansiva.

De Terwangne, C. (2009). Is a Global Data Protection Regulatory Model Possible? En S. Gutwirth, Y. Poullet, P. De Hert, C. De Terwangne y S. Nouwt (Eds.), *Reinventing data protection?* (pp. 175-189). Dordrecht: Springer.

Delpiazzo, C. (2007). El principio de seguridad jurídica en el mundo virtual. *Revista de Derecho de la Universidad de Montevideo, 6*(11). Recuperado el 4 de abril de 2019 de http://revistaderecho.um.edu.uy/wp-content/uploads/2012/10/DERECHO-11.pdf

Departamento de Justicia de los Estados Unidos. (s.f.) *Freedom of information Act, 5 U.S.C. § 552ª, Ley de libertad de información de 1966.* Recuperado el 27 de abril de 2019 de https://www.justice.gov/oip/freedom-information-act-5-usc-552

Departamento de Seguridad Nacional de los Estados Unidos. (s.f.). *Privacy Act, 5 U.S.C. § 552ª, Ley de Privacidad de Estados Unidos de Norteamérica de 1974.* Recuperado el 12 de mayo de 2019 de https://www.uscis.gov/about-us/freedom-information-and-privacy-act-foia/privacy-act-1974

Derecho Chile. (s.f.). *Sentencia 209/83 del Tribunal Constitucional Federal*

Alemán de 15 de diciembre de 1983, Ley del Censo. Recuperado el 17 de abril de 2019 de 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. (s.f.). *Ley de Protección de Datos Personales de Uruguay, Nro. 18.331 de 2008.* Recuperado el 25 de marzo de 2019 de https://www.impo.com.uy/bases/leyes/18331-2008

Dirección Nacional de Impresiones y Publicaciones. (s.f.). *Reglamentación de la ley Nro. 18.331, relativo a la protección de datos personales, Uruguay de 2009, Decreto Nro. 414/009.* Recuperado el 25 de marzo de 2019 de https://www.impo.com.uy/bases/decretos/414-2009

Dirección Nacional de Registro de Datos Públicos. (2019). *Anteproyecto de la Ley Orgánica de Protección de datos Personales de 28 de mayo de 2019.* Recuperado el 30 de mayo de 2019 de http://www.datospublicos.gob.ec/wp-content/uploads/downloads/2019/05/Anteproyecto-de-Ley-Org%C3%A1nica-de-Protecci%C3%B3n-de-Datos-Personales.pdf

Enríquez, L. (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*, 27. Recuperado el 26 de marzo de 2019 de http://repositorio.uasb.edu.ec/bitstream/10644/5945/1/05-TC-Enriquez.pdf

Estrada, J., Estrada, J., Rodríguez, A., y Tipantuña, C. (2015). Ecuador y la Privacidad en Internet: Una Aproximación Inicial. *Revista Politécnica,*

36(1). Recuperado el 28 de marzo de 2019 de http://www.revistapolitecnica.epn.edu.ec/images/revista/volumen36/tomo1/EcuadorylaPrivacidadenInternetUnaAproximacionInicial.pdf

Eur-Lex. (s.f.). *Caso Lindqvist vs. Gäta hovärtt, sentencia de 6 de noviembre de 2003 del Tribunal de Justicia de la Unión Europea.* Recuperado el 15 de abril de 2019 de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN

Eur-Lex. (s.f.). *Caso Schrems vs. Data Protection Commissioner, sentencia de 6 de octubre de 2015, asunto C-362/14 del Tribunal de Justicia de la Unión Europea, Gran Sala.* Recuperado el 18 de marzo de 2019 de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62014 CJ0362&from=ES

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

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

Eur-Lex. (s.f.). *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*. Recuperado el 4 de mayo de 2019 de https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

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

Fedexport. (2019). Reporte Mensual de Comercio Exterior. *Expordata.* Recuperado el 25 de mayo de 2019 de http://www.fedexpor.com/wp-content/uploads/2019/02/Expordata-Especial-2018.pdf.

Ferrajoli, L. (2001). *Los fundamentos de los derechos fundamentales.* Madrid: Trotta.

Foro de Cooperación Económica Asia-Pacífico. (s.f.). *Marco de privacidad de la APEC de 2004*. Recuperado el 18 de marzo de 2019 de https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

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

Garrido, D. (1991). El proyecto de Ley de regulación del tratamiento automatizado de los datos de carácter personal: la excepcionalidad como norma. *Jueces para la democracia*, 13. Recuperado el 25 de marzo de 2019 de https://dialnet.unirioja.es/descarga/articulo/2528793.pdf

Garriga, A. (2016). *Nuevos retos para la protección de datos personales en la era del Big Data y la computación ubicua.* Madrid: DYKINSON.

Gibello, V. y Moritz, M. (2017). El Reglamento Europeo (UE) 2016/679: análisis de un claroscuro. *Foro*, 27. Recuperado el 25 de marzo de 2019 de

http://repositorio.uasb.edu.ec/bitstream/10644/5948/1/08-TC-Moritz-Gibello.pdf

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

Gobierno de Brasil. (s.f.). *Ley General de Protección de Datos de Brasil, Nro. 17.309. de 2018.* Recuperado el 14 de mayo de 2019 de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Gobierno de México. (s.f.). *Constitución Política de los Estados Unidos Mexicanos de 5 de febrero de 1917*. Recuperado el 20 de mayo de 2019 de http://www.sct.gob.mx/JURE/doc/cpeum.pdf

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

Grande, M. (2016). Transferencia internacional de datos personales desde España a países iberoamericanos. *Informática y Derecho, 1*(1). Recuperado el 17 de abril de 2019 de https://docs.wixstatic.com/ugd/fe8db5_a143e0cda3b44d5998a5c1fe4c70 c8 28.pdf

Gregorio, C. (2005). *Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina.* [versión electrónica]. Recuperado el 20 de marzo de 2019 de https://archivos.juridicas.unam.mx/www/bjv/libros/3/1407/12.pdf

Guasch Portas, V. (2012). La transferencia internacional de datos de carácter personal. *RDUNED*, 11. Recuperado el 20 de abril de 2019 de http://revistas.uned.es/index.php /RDUNED/article/view/11139/10667

Guzmán, M. (2013). El derecho fundamental a la protección de datos personales en México: *análisis desde la influencia del ordenamiento jurídico español* (Tesis Doctoral). Recuperado el 16 de marzo de 2019 de https://eprints.ucm.es/22817/1/T34727.pdf

Honorable Cámara de Diputados. (s.f.). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México de 2010.* Recuperado el 30 de abril de 2019 de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Honorable Cámara de Diputados. (s.f.). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de México de 2017.* Recuperado el 14 de mayo de 2019 de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Honorable Cámara de Diputados. (s.f.). *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México de 2011.* Recuperado el 10 de mayo de 2019 de http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

Infoleg. (s.f.). *Reglamentación de la ley Nro. 25.326, relativo a la protección de datos personales de Argentina de 2001, Decreto Nro. 1558/2001.* Recuperado el 25 de marzo de 2019 de http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/texact.htm

Legisalud. (s.f.). *Constitución de la Nación Argentina de 23 de agosto de 1994.* Recuperado el 10 de abril de 2019 de http://test.e-legis-

ar.msal.gov.ar/leisref/public/showAct.php?id=877

Levin, A. y Nicholson, M. (2005). Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground. *University of Ottawa law & technology journal*, 357. Recuperado el 17 de marzo de 2019 de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=894079

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (2002). Registro Oficial 557, Suplemento, de 17 de abril de 2002. Última modificación: 10 de febrero de 2014.

Ley de Seguridad Pública y del Estado. (2009). Registro Oficial 35, Suplemento, de 28 de septiembre de 2009. Última modificación: 21 de junio de 2017.

Ley de Seguridad Social. (2001). Registro Oficial 465, Suplemento, de 30 de noviembre de 2001. Última modificación: 30 de abril de 2019.

Ley General de los servicios postales. (2015). Registro Oficial 603, Suplemento, de 07 de octubre de 2015.

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. (2009). Registro Oficial 52, Suplemento, de 22 de octubre de 2009. Última modificación: 10 de enero de 2018.

Ley Orgánica de Gestión de la Identidad y Datos Civiles. (2016). Registro Oficial 684, Suplemento, de 04 de febrero de 2016. Última modificación: 14 de marzo de 2018.

Ley Orgánica de la Salud. (2006). Registro Oficial 423, Suplemento, de 22 de diciembre de 2006. Última modificación: 23 de octubre de 2018.

Ley Orgánica de Movilidad Humana. (2017). Registro Oficial 938, Suplemento, de 06 de febrero de 2017. Última modificación: 06 de mayo de 2019.

Ley Orgánica de Telecomunicaciones. (2015). Registro Oficial 439, Suplemento, de 18 de febrero de 2015. Última modificación: 7 de julio de 2017.

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

Ley Orgánica del Sistema Nacional de Registro de Datos Públicos. (2010). Registro Oficial 162, Suplemento, de 31 de marzo de 2010. Última modificación: 29 de diciembre de 2017.

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

López, L. (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. Recuperado el 25 de marzo de 2019 de https://www.uria.com/documentos/publicaciones/5315/documento/art03.pdf?id=6965

Lucena, I. (2012) La protección de la intimidad en la era tecnológica: hacia un re conceptualización. *Revista Internacional del Pensamiento Político*, (7). Recuperado el 1 de mayo de 2019 de http://www.pensamientopolitico.org/Descargas/RIPP07117144.pdf

Maqueo, M., Moreno, J., y Recio, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho Valdivia, 30*(1). Recuperado el 30 de abril de 2019 de https://scielo.conicyt.cl/pdf/revider/v30n1/art04.pdf

Naranjo, L. (2017). El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador. *Foro*, 27. Recuperado el 15 de marzo de 2019 de http://repositorio.uasb.edu.ec/bitstream/10644/5946/1/06-TC-Naranjo.pdf

Oficina del Asesor Jurídico de Revisión de la Cámara de Representantes de los Estados Unidos. (s.f.). *Right to Financial Privacy Act, 12 U.S.C. §§ 3401/342, Ley de libertad de información de 1978.* Recuperado el 19 de abril de 2019 de http://uscode.house.gov/view.xhtml?path=/prelim@title12/chapter35&edition=prelim

Ordóñez, L. (2017). La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración. Foro, 27. Recuperado el 14 de abril de 2019 de http://repositorio.uasb.edu.ec/bitstream/10644/5947/1/07-TC-Ordo%C3%B1ez.pdf

Organización de Estados Americanos. (s.f.). *Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la OCDE de 1980.* Recuperado el 5 de abril de 2019 de http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf

Organización de Estados Americanos. (s.f.). *Ley de Protección de Datos Personales de Argentina, Nro. 25.326 de 2000.* Recuperado el 25 de marzo de 2019 de https://www.oas.org/juridico/PDFs/arg_ley25326.pdf

Ornelas, L. (2008). Transferencias internacionales de datos personales: su protección en el ámbito del comercio internacional y de seguridad

nacional. En E. Ferrer y A. Zaldívar (Coords.), *Procesos constitucionales de la libertad* (pp. 731-758). México: Marcial Pons.

Ortega, A. (2017). Transferencia Internacional de Datos de Carácter Personal: del Safe Harbour al Privacy Shield. *Lex Mercatoria,* 4. Recuperado el 25 de marzo de 2019 de http://revistas.innovacionumh.es/index.php?journal=lexmercatoria&page=article&op=view&path%5B%5D=1093&path%5B%5D=208

Ortega, A. y Domenech, J. (2018). Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea. *Revista de la Facultad de Derecho* (44). Recuperado el 28 de marzo de 2019 de https://dx.doi.org/10.22187/rfd2018n44a2

Patterson Belknap. (2018). *California Consumer Privacy (CCPA), Ley de privacidad del consumidor de California*. Recuperado el 30 de mayo de 2019 de https://www.pbwt.com/content/uploads/2018/06/California-Consumer-Privacy-Act1.pdf

Puccinelli, O. (1999). *El habeas data en Indoiberoamérica*. Bogotá: Temis.

Pulido, C. (2015). Derechos fundamentales. En J. Fabra y A. Nuñez (Eds.), Enciclopedia de filosofía y teoría del derecho (pp. 1571-1594). México: UNAM.

Rebollo, L. (2008). Vida privada y protección de datos en la Unión Europea. Madrid: Dykinson.

Rebollo, L. y Serrano, M. M. (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*. Recuperado el 15 de marzo de 2019 de http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

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

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

Reglamento a la Ley Orgánica de Movilidad Humana. (2017). Decreto Ejecutivo 111. Registro Oficial 55, de 10 de agosto de 2017. Última modificación: 20 de diciembre de 2018.

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

Reglamento General a la Ley General de los Servicios Postales. (2016). Decreto Ejecutivo 1156. Registro Oficial 854, de 04 de octubre de 2016.

Reglamento General a la Ley Orgánica de Telecomunicaciones. (2016). Decreto Ejecutivo 864. Registro Oficial 676, Suplemento, de 25 de enero de 2016.

Remolina, N. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?. *Revista Colombiana de Derecho Internacional*, 16. Recuperado el 15 de mayo de 2019 de

https://revistas.javeriana.edu.co/index.php/internationallaw/article/view/13847

Remolina, N. (2015). *Recolección internacional de datos personales: un reto del mundo post-internet* [versión electrónica]. Recuperado el 17 de abril de 2019 de https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Remolina-N-2015-RIDP-post-internet-CAP-PRELIMINAR.pdf

Remolina, N., Tenorio, M., y Quintero, G. (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.

Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum Jus, 8*(1). Recuperado el 19 de mayo de 2019 de https://editorial.ucatolica.edu.co/ojsucatolica/revistas_ucatolica/ index.php/ Juridica/article/viewFile/652/670

Saltor, C. (2013). *La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina* (tesis doctoral). Recuperado el 18 de marzo de 2019 de https://eprints.ucm.es/22832/1/T34731.pdf

Sánchez Gonzáles, M. (2015). *Implicaciones Institucionales de la Ley de Protección de Datos* (Tesis Doctoral). Recuperado el 15 de abril de 2019 de https://riuma.uma.es/xmlui/bitstream/handle/10630/11792/TD_SANCHEZ_GONZALEZ_Maria_Belen.pdf?sequence=1&isAllowed=y

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

Santos, J. (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*, 2. Recuperado el 28 de mayo de 2019 de https://www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf

Sanz, L. (2008). Principios de la Protección de Datos. En C. Lesmes (Coord.), *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia* (pp. 138-162). Valladolid: LEX NOVA.

Torres, B. (2010). *Proyecto de Ley Orgánica de Protección de Datos Personales* (Tesis de maestría). Recuperado el 18 de mayo de 2019 de http://dspace.ucuenca.edu.ec/bitstream/123456789/2660/1/tm4350.pdf

Tribunal Constitucional Español. (s.f.). *Sentencia 292/2000 del Tribunal Constitucional Español de 30 de noviembre de 2000.* Recuperado el 16 de abril de 2019 de http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276#complete_resolucion&completa

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

Uría, E. (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*, 53. Recuperado el 14 de mayo de 2019 de http://dx.doi.org/10.18042/cepc/rdce.53.07

Valverde, A. (2013). Protección de datos de carácter personal y derechos de información de los representantes de los trabajadores. *Temas Laborales*, 118. Recuperado el 6 de abril de 2019 de http://www.juntadeandalucia.es/empleo/anexos/ccarl/33_1392_3.pdf

Villalba, A. (2017). Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa. *Foro,* 27. Recuperado el 18 de abril de 2019 de http://repositorio.uasb.edu.ec/bitstream/10644/5944/1/04-TC-Villalba.pdf

Warren, S. y Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220. Recuperado el 30 de abril de 2019 de http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

World Intellectual Property Organization. (s.f.). *Constitución de la República Federativa de Brasil de 5 de octubre de 1988.* Recuperado el 18 de mayo de 2019 de https://www.wipo.int/edocs/lexdocs/laws/es/br/br117es.pdf

Zaballos, E. (2013). *La Protección de Datos Personales en España: Evolución Normativa y Criterios de Aplicación* (Tesis Doctoral). Recuperado el 18 de mayo de 2019 de https://eprints.ucm.es/22849/1/T34733.pdf

ANEXOS

Anexo 1. Explicación del desarrollo normativo de la protección de datos personales en el 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 información pública 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 a 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	Confidencialidad de los datos personales de las personas ecuatorianas en el exterior, cualquiera que sea u 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). Según el Art. 92 toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a

	personal que se encuentren en los archivos de las instituciones del Ecuador en el exterior. (Art. 44).	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, el 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 licito.	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 sólo 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 éste autorice o por disposición de este Código. (Art. 352). El Registro de datos crediticios es utilizada 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	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).

	del espectro radioeléctrico.	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, rectificabilidad, 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)	Regula 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.: a) 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	Regula la optimización de trámites administrativos, regular su simplificación y	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

Administrativos (2018)	reducir sus costos de gestión.	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: normativa ecuatoriana que regula la protección de datos personales hasta la actualidad.