UNIVERSIDAD NACIONAL
SISTEMA DE ESTUDIOS DE POSGRADO
CENTRO INTERNACIONAL DE POLÍTICA ECONÓMICA
PARA EL DESARROLLO SOSTENIBLE
POSGRADO EN GERENCIA DEL COMERCIO INTERNACIONAL

DESAFÍOS DE LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES ENTRE COSTA RICA Y LA UNIÓN EUROPEA: CONSIDERACIONES NORMATIVAS PARA LA FACILITACIÓN DEL COMERCIO

MARÍA PAULA GAMBOA QUIRÓS

HEREDIA, COSTA RICA
MAYO, 2024

Trabajo Final de Graduación sometido a consideración del Tribunal Examinador de la Maestría en Gerencia del Comercio Internacional para optar por el grado de Magíster

DESAFÍOS DE LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES ENTRE COSTA RICA Y LA UNIÓN EUROPEA: CONSIDERACIONES NORMATIVAS PARA LA FACILITACIÓN DEL COMERCIO

MARÍA PAULA GAMBOA QUIRÓS

MIEMBROS DEL TRIBUNAL EXAMINADOR

Marco Otoya Chavarría
Director Programa Docente

Suyen Alonso Ubieta
Tutor (a)

Donald Miranda Montes
Miembro del Comité Asesor

Ana Karen Cortés Víquez
Miembro del Comité Asesor

María Paula Gamboa Quirós
Sustentante

Índice de contenido

Índice de figuras

Índice de tablas

Resumen

En un mundo cada vez más globalizado y digitalizado, la transferencia internacional de datos se ha convertido en un componente fundamental del comercio internacional. Por ello, este trabajo se enfoca en estudiar las consideraciones normativas que deben existir para que la Unión Europea le conceda a Costa Rica un nivel adecuado de protección de datos personales que facilite la transferencia internacional de éstos y convierta a Costa Rica en un puerto seguro para la facilitación del comercio. Esta investigación adopta un enfoque exploratorio, dada la escasez de evidencia disponible sobre el tema. Consecuentemente, la información se recopiló mediante el análisis documental y las entrevistas a expertos. Entre los principales hallazgos se destacan una serie de desafíos que Costa Rica debe afrontar si busca lograr la adecuación. Así, estos incluyen la necesidad de fortalecer las capacidades de la Prodhab, llevar a cabo una reforma integral de la Ley No. 8968 y promover la concienciación entre empresas, instituciones y la sociedad civil sobre la importancia de la protección de datos. Por otro lado, se resaltan las implicaciones que enfrentaría el país en caso de no lograr la adecuación, como la pérdida de mercados y competitividad en el ámbito internacional.

Palabras clave: datos personales, transferencia internacional de datos personales, decisión de adecuación, Unión Europea, Costa Rica.

Abstract

In an increasingly globalized and digitalized world, the international transfer of data has become a fundamental component of international trade. Thus, this paper focuses on studying the regulatory considerations that must exist for the European Union to grant Costa Rica an adequate level of personal data protection to facilitate the international transfer of the data and turn Costa Rica into a safe harbor for trade facilitation. This research adopts an exploratory approach, given the scarcity of available evidence on the subject. Information was gathered through documentary analysis and expert interviews. Among the main findings, there are a number of challenges that Costa Rica must address if it is to achieve adequacy. These include the need to strengthen the capacities of Prodhab, carry out a comprehensive reform of the Bill No. 8968 and promote awareness among companies, institutions and civil society about the importance of data protection. On the other hand, the implications that the country would face in case of not achieving compliance are highlighted, such as the loss of markets and competitiveness in the international arena.

Key words: personal data, international transfer of personal data, adequacy decision, European Union, Costa Rica.

Introducción

En la era digital actual, el flujo de información digital se ha convertido en uno de los pilares que impulsa el comercio. Por ello, tanto Estados como empresas de todo el mundo participan activamente en la transferencia diaria de datos. Este intercambio masivo de datos plantea desafíos significativos en un contexto donde las fronteras nacionales y las normativas dispares entre países aún perduran. En este contexto, la Unión Europea (UE) ha armonizado su legislación con el fin de que la transferencia de datos personales entre los países miembros se lleve a cabo con un adecuado nivel de seguridad. Por tal razón, cuando las transferencias internacionales se llevan a cabo para un tercer país, este debe ofrecer garantías comparables a las de la UE.

En este sentido, esta investigación busca analizar los desafíos que Costa Rica debe enfrentar y las consideraciones normativas que deben existir para que la UE le conceda un nivel adecuado de protección de datos personales que lo convierta en un puerto seguro en pro de la facilitación comercial. El propósito es brindar un punto de partida acerca del tema desde una perspectiva del comercio internacional. Por consiguiente, dada la escasez de evidencia disponible sobre el tema, esta investigación opta por un enfoque exploratorio. En consecuencia, se recopiló información a través del análisis documental y de cinco entrevistas a expertos.

La investigación se divide en cinco capítulos, el primero incluye los antecedentes, la justificación, el planteamiento del problema y los objetivos. Por su parte, el segundo capítulo integra el marco conceptual y el marco metodológico. En el tercero se describe el marco institucional internacional y nacional en materia del flujo transfronterizo de datos personales. Por otro lado, en el cuarto capítulo se examina el flujo transfronterizo de datos personales desde la UE hacia un tercer país, las decisiones de adecuación y los mecanismos alternativos. Por último, en el capítulo cinco, se analizan los desafíos institucionales y normativos de Costa Rica en cuanto a la transferencia internacional de datos personales, recomendaciones y perspectivas globales futuras.

CAPÍTULO I: ANTECEDENTES Y JUSTIFICACIÓN

1.1. Antecedentes

La protección de datos personales comenzó a tomar relevancia durante la segunda mitad del siglo XX, luego de la Segunda Guerra Mundial, dada la necesidad de protección de la dignidad humana y la preocupación por la intimidad, así como el impacto social y económico producido por los crímenes cometidos contra la humanidad. Es así como en el Reglamento (UE) 2016/679[1] se plasma en el considerando 158 que indica:

> Los Estados miembros también debe estar autorizados a establecer el tratamiento ulterior de datos personales con fines de archivo, por ejemplo, a fin de ofrecer información específica relacionada con el comportamiento político bajo antiguos regímenes de Estados totalitarios, el genocidio, los crímenes contra la humanidad, en particular el Holocausto, o los crímenes de guerra.

Lo anterior, generó la necesidad de normar la transmisión y el tratamiento de estos datos para garantizar su protección. En 1948, la Asamblea General de las Naciones Unidas adopta la Declaración Universal de Derechos Humanos, en donde se establecen los derechos fundamentales que deben protegerse. En el artículo 12 de dicha Declaración se decreta que:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Si bien es cierto, aun cuando este artículo no se refiere explícitamente a la protección de los datos personales, se entiende como un derecho que se deriva de este, debido a que en el momento en que se adopta la Convención, no existía una necesidad real de normar la protección de datos personales. Ahora bien, es a partir del auge de la era digital en la década de los 2000, que se originan los derechos digitales[2], entre los que se incluye el derecho a la privacidad y a

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD).

[2] De acuerdo con el Pacto Mundial de las Naciones Unidas (2022), los derechos digitales "(...) fomentan un modelo de transformación digital que refuerce la dimensión humana. Éstos tienen por objetivo final garantizar el acceso a Internet a todas las personas para cerrar la brecha digital, y promover un uso correcto de la red como un bien común de toda la humanidad".

la protección de datos. Estos derechos son entendidos como una extensión de los recogidos en la Declaración mencionada anteriormente (Pacto Mundial de las Naciones Unidas, 2022).

Con el advenimiento del internet y la globalización económica, el tratamiento de los datos personales también ha permeado el comercio internacional pues, los flujos transfronterizos de datos personales se han convertido en un elemento esencial. Al respecto Yakovleva (2022) afirma que "El uso comercial de los datos personales potencia el comercio digital y contribuye al crecimiento económico[3]" (p.1). En 1980, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) entendió la importancia de la transferencia internacional de datos en el comercio, es así como declaró que los países debían "evitar la elaboración de leyes, políticas y prácticas destinadas a proteger la privacidad y las libertades individuales que pudieran crear obstáculos al flujo transfronterizo de datos personales excediendo los requisitos para tal protección" (p. 8).

El concepto transferencia internacional de datos ha contado con diferentes denominaciones en las regulaciones que han emergido a lo largo del tiempo: flujos transfronterizos de datos personales, transferencia de datos personales a países terceros, movimiento internacional de datos, entre otros. Para 1980, la OCDE ya hacía referencia al término flujos transfronterizos de datos personales y lo entendía como aquellos desplazamientos de datos personales que se efectuaban fuera de las fronteras nacionales. Además, esta organización instó a los países pertenecientes a la organización a crear un marco institucional (leyes, políticas y prácticas) que protegieran la privacidad y las libertades individuales, para que así no se obstaculizara el tránsito de estos datos (Polo, 2021).

En la esfera internacional, el primer instrumento jurídicamente vinculante surgió en lo referente a la protección de datos fue el Convenio 108 de 1981 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (sustituido en la actualidad por el Convenio 108+[4] del año 2018). Este buscaba enlazar

[3] Traducción libre. Texto original: "the commercial use of personal data empowers digital trade and contributes to economic growth".

[4] Nombre Completo: Convenio No. 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, modificado por el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE No. 108), adoptado por el Comité de Ministros en su Sesión No. 128ª el 18 de mayo de 2018.

la circulación transfronteriza de los datos y su debida protección, en el artículo 1 de esta normativa se establece que su objeto y fin es:

> (...) garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (Consejo de Europa, 1981, p.2).

Adicionalmente, en el artículo 12 del Convenio 108 de 1981, se determina que los flujos transfronterizos de datos de carácter personal se refieren a "las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento" (Consejo de Europa, p.6).

Posteriormente, a partir de la iniciativa marcada por el Convenio 108, la UE elaboró la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 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. El objeto de dicha normativa se determina en el artículo 1 apartado 1 y 2 de la legislación donde se indica que los Estados miembros deben garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, en especial, del derecho a la intimidad; adicionalmente la Directiva señala que los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre ellos.

Por ello, se entiende que el fin de este instrumento jurídico era enlazar la protección de las personas en lo referente a sus datos personales y a la libre circulación de los mismos de un Estado miembro a otro. Adicionalmente, esta norma reguló la transferencia de datos personales a países terceros en el capítulo IV, en donde se señala que los Estados miembros podrán efectuar la transferencia de datos personales hacia un país tercero, únicamente si este último garantiza un nivel de protección adecuado[5].

A pesar de que ni la Directiva 95/46/CE ni el RGPD definen qué se entiende por un nivel de protección adecuado, el Tribunal de Justicia de la Unión Europea (TJUE) se pronunció en lo referente a este concepto el 6 de octubre de 2015 en la sentencia con asunto C-362/14

[5] Artículo 25.1 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

donde anuló el Acuerdo de Puerto Seguro (*Safe Harbor Agreement)* entre la UE y Estados Unidos. El TJUE señaló en el apartado 73 que:

> (...) el término «adecuado»[6] que figura en el artículo 25, apartado 6, de la Directiva 95/46 significa que no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión. Sin embargo, como ha manifestado el Abogado General en el punto 141 de sus conclusiones, debe entenderse la expresión «nivel de protección adecuado» en el sentido de que exige que ese tercer país 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 la Unión por la Directiva 95/46.

Así, lo expuesto, implica que los terceros países deben contar con un nivel de protección que sea en esencialmente equivalente al proporcionado por la legislación europea. No obstante, tal y como lo menciona Recio (2019) "(...) una definición o un planteamiento unilateral da lugar a un importante desequilibrio, ya que se impone un estándar y no se atiende a todas las cuestiones que pueden darse en la práctica" (p. 214).

En cuanto a Costa Rica, se puede mencionar como antecedente sobre la protección de los datos personales el artículo 24 de la Constitución Política que garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones; donde se estipula que "Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República". Si bien, este artículo no involucra el derecho a la protección de datos personales, se ha entendido tradicionalmente como un derecho derivado (París, 2020).

Aunado a lo anterior, en 2011 se adoptó la Ley de Protección de la Persona frente al tratamiento de sus datos personales No. 8968, esta tiene como objetivo:

> (...) garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto

[6] En comercio internacional, el homólogo del término adecuado, es el de trato nacional. El trato nacional lo define la OMC (s.f.) como "(...)igual trato para nacionales y extranjeros. Las mercancías importadas y las producidas en el país deben recibir el mismo trato, al menos después de que las mercancías extranjeras hayan entrado en el mercado".

al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Por otra parte, la Ley No. 8968 incluye en el capítulo III, la transferencia de datos personales e indica en el artículo 14 que se podrán transferir datos ubicados en bases de datos públicas o privadas únicamente cuando el titular autoriza expresamente la transferencia; sin embargo, cabe destacar que este artículo no regula la transferencia internacional de datos personales.

Actualmente, existe en la corriente legislativa el Proyecto de Ley No. 23.097: Ley de Protección de Datos Personales, propuesto por el diputado Eliécer Feinzaig, quién es el presidente y jefe de fracción del Partido Liberal Progresista (PLP)[7]. Este Proyecto plantea una reforma legal integral al marco regulatorio en materia de protección de datos personales e introduce en el capítulo V donde se regulan las transferencias internacionales de datos personales y se hace referencia a los supuestos en los cuáles se podrán realizar dichas transferencias.

Ahora bien, pese a que la vinculación entre las transferencias internacionales de datos, la protección de datos personales y el comercio puede no ser tan explícita, sí existe y el nexo es estrecho. Este vínculo se hace más evidente después de 1994, cuando la mayoría de las naciones acordaron crear la Organización Mundial del Comercio (OMC) y con ello la liberalización del comercio de servicios; sin embargo en aquel momento nadie se percató (quizá aún muchos no dimensionan lo sucedido) que al liberalizar el comercio de servicios permitía que todos, potencialmente se convirtieran en un exportador o importador de bienes y servicios (Ariel, 2017). Así Wu (2006) establece que "De ahí que, casi por accidente, la OMC se haya colocado en una posición de supervisión de la mayoría de las leyes y prácticas nacionales que regulan Internet"[8] (p. 264).

Hoy en día, el mundo se encuentra globalizado y digitalizado; por lo que, no es un secreto que el Internet y otras tecnologías de la información y la comunicación (TICs) propician e impulsan el surgimiento de modelos de negocio que transforman la manera de producir y de comercializar bienes y servicios. Al respecto, Casalini y López-Gónzalez (2019) afirman que:

[7] El PLP nace el 27 de febrero del 2016.

[8] Traducción libre. Texto original: "Hence, almost by accident, the WTO has put itself in an oversight position for most of the national laws and practices that regulate the Internet".

> En esta era digital, el comercio y la producción dependen en gran medida de la circulación, el almacenamiento y la utilización de información digital (datos), cada vez más transfronteriza. Los datos permiten la coordinación de los procesos de producción internacionales a través de las cadenas de valor mundiales (CVM), ayudan a las pequeñas empresas a llegar a los mercados mundiales, son un activo con el que se puede comerciar, un conducto para la prestación de servicios y un componente clave para la automatización en la facilitación del comercio (p. 8)[9].

A pesar de que el Internet y las TICs ofrecen oportunidades para las empresas y los países, este intercambio masivo de datos ha despertado la preocupación de gobiernos y de ciudadanos sobre los efectos negativos de la gran cantidad de información que se recolecta, se utiliza y se comercializa, en muchas ocasiones sin el consentimiento del titular de los datos; especialmente si se hace énfasis en los datos de carácter personal. Esta situación, plantea desafíos considerables para las políticas nacionales e internacionales en un mundo donde aún se mantienen las fronteras y las distintas normativas entre países (Casalini y López-Gónzalez, 2019).

Es así como este trabajo se enfoca en estudiar las consideraciones normativas que deben existir para que la Unión Europea le conceda a Costa Rica (región-país) un nivel adecuado de protección de datos personales que facilite la transferencia internacional de estos datos y convierta a Costa Rica en un puerto seguro para la facilitación del comercio. El propósito es ofrecer un punto de partida sobre la materia desde una óptica del comercio internacional y los eventuales retos que esto conlleva.

1.2. Justificación del problema

En un mundo globalizado como el actual, la transmisión de datos resulta vital, si se toma en consideración que tanto Estados como empresas alrededor del mundo transfieren millones de datos diariamente a diferentes usuarios. En este sentido, nuevas tecnologías han impulsado las transferencias internacionales de datos personales, mismas que deben ser reguladas y deben contemplar los siguientes elementos: a) la protección de datos y la intimidad,

[9] Traducción libre. Texto original: "In this digital age, trade and production are heavily dependent on moving, storing and using digital information (data), increasingly across borders. Data enables the coordination of international production processes through global value chains (GVCs), it helps small firms reach global markets, it is an asset that can itself be traded, a conduit for delivering services and a key component for automation in trade facilitation".

b) el interés público del Estado, c) la actividad de las empresas a nivel internacional y d) la libertad de información y comunicación (Polo, 2021).

Tal y como se mencionó anteriormente, el flujo de datos se ha convertido en una parte inherente del comercio internacional. Por consiguiente, los flujos transfronterizos de datos han constituido uno de los más importantes desafíos en el tratamiento de la información personal. Lo anterior, se debe a la disparidad de ordenamientos jurídicos, las circunstancias del mercado, la competencia territorial y la carencia o inexistencia de normas vinculantes. De acuerdo con Cordero (2019) "en un contexto como el actual, las transferencias internacionales de datos personales resultan esenciales para el desarrollo de los intercambios comerciales y para la prestación de los servicios en línea" (p. 51).

Cabe destacar que las transferencias internacionales de datos personales traen consigo un alto riesgo en cuanto al derecho de autodeterminación informativa[10] debido a que: a) los datos pueden perderse o ser alterados, b) el alcance internacional supone que el objeto de control se traslade fuera de las fronteras, c) se elaboren ficheros con información de la ciudadanía de múltiples Estados (Aberasturi, 2011).

Por ello, estudiar la transferencia internacional de datos personales entre Costa Rica y la Unión Europea desde la perspectiva de un puerto seguro y de la facilitación del comercio es sumamente importante porque: a) aporta elementos de los cuáles hay poca evidencia en los países en desarrollo, en el caso de Costa Rica es casi inexistente, la evidencia teórica que se encuentra es principalmente de Colombia[11], b) la temática es actual y relevante en el contexto de la digitalización y la globalización, y c) es necesario comprender este tema de manera integral con el fin de reforzar el marco regulatorio de protección de datos personales, fomentar los intercambios comerciales y generar una mayor sensibilización en la ciudadanía.

1.3. Planteamiento del problema

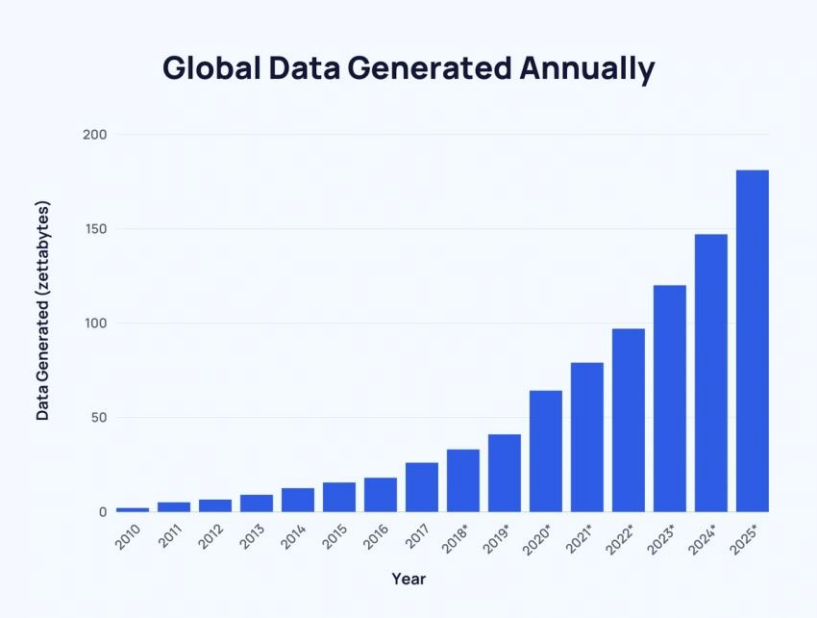
Hoy más que nunca, los datos personales son un activo de valor económico, se les ha denominado el petróleo del siglo XXI y la moneda del nuevo milenio (Shwartz, 2004); también

[10] La autodeterminación informativa incluye el derecho fundamental de las personas a decidir sobre quién, cuándo y bajo cuáles circunstancias otras personas tienen acceso a sus datos, así como el derecho a conocer la información que conste sobre ella en las bases de datos y el derecho a que esta información sea rectificada, actualizada, complementada o suprimida, cuando sea incorrecta (Asamblea Legislativa de Costa Rica, 2010, párr. 8).

[11] Nelson Remolina-Angarita, ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 International Law, Revista Colombiana de Derecho Internacional, 489-524 (2010).

se ha afirmado que los datos son la savia del comercio internacional (Casalini y López-González, 2019). De acuerdo con Duarte (2023) "(...) se estima que el 90% de los datos mundiales se ha generado tan sólo en los dos últimos años[12]". A continuación, en la figura 1, se muestra el comportamiento de los datos globales generados anualmente y su pronóstico hacia 2025. Esta figura evidencia el crecimiento exponencial de los datos generados en los últimos años y, "(...) se espera que los 120 zettabytes generados en 2023 aumenten más de un 150% en 2025, alcanzando los 181 zettabytes"[13].

Figura 1. Datos globales generados anualmente, 2010-2025



Fuente: Tomado de Duarte (2023)

En este sentido, empresas de todos los tamaños y sectores emplean datos en sus operaciones diarias. Por ejemplo, Casalini y López-González (2019) señalan que las multinacionales requieren "(...) en gran medida de los flujos de datos transfronterizos para sus operaciones cotidianas; utilizan los datos de sus filiales en todo el mundo para un gran número de tareas internas, o de back office, e incluso para decisiones rutinarias" (p. 6). A su vez, la Comisión Europea (2017) recalca que los intercambios comerciales son cada vez más dependientes de la circulación de datos personales y menciona que "(...) en la era digital es

[12] Traducción libre. Texto original: "it is estimated that 90% of the world's data was generated in the last two years alone".

[13] Traducción libre. Texto original: "The 120 zettabytes generated in 2023 are expected to increase by over 150% in 2025, hitting 181 zettabytes".

imprescindible que el fomento de estrictas normas de protección de datos vaya acompañado de la facilitación del comercio internacional" (p. 7).

Al respecto, el Reglamento (UE) 2016/679 establece un régimen que involucra un conjunto de instrumentos que posibilita la circulación de datos: a) las transferencias internacionales basadas en una decisión de adecuación (artículo 45), b) transferencias mediante garantías adecuadas (artículo 46) y c) supuestos de normas corporativas o vinculantes (artículo 47). Cabe destacar que como principio general, las transferencias de datos personales a terceros países sólo podrán efectuarse si se garantiza un nivel adecuado de protección de tratamiento.

Así las cosas, para los países de la Unión Europea "(...) la integración económica y social ha implicado notoriamente un aumento de los flujos transfronterizos de datos personales entre los agentes públicos y privados" (Matus, 2010, p. 1). Esta situación, es posible dada la legislación existente armonizada, que permite que la transferencia de datos personales entre los países miembros se efectúe con un adecuado nivel de seguridad. Por tal motivo, cuando las transferencias internacionales se llevan a cabo fuera del Espacio Económico Europeo (EEE)[14], el tercer país, quien es el importador del dato debe ofrecer garantías de protección comparables a las de la Directiva Europea.

En este sentido, se espera que no solo exista una legislación que integre los principios básicos de protección de la regulación Europea, sino que además, se busca que existan los medios adecuados que permitan el correcto ejercicio de los derechos. Lo anterior, significa que debe existir de un órgano de control que cuente con la competencia y las facultades de fiscalización y sanción en lo referente a la protección de los datos personales. Por lo tanto, no lograr una decisión de adecuación puede acarrear efectos económicos negativos de gran alcance.

En primer lugar, las empresas se enfrentarían a costos adicionales significativos al tener que implementar medidas específicas para garantizar la protección de datos en ausencia de un marco legal claro y armonizado. Estos costos podrían derivarse de la necesidad de conseguir certificaciones, contratar expertos en protección de datos, adaptar sistemas informáticos o enfrentar sanciones por el incumplimiento de la legislación Europea. Adicionalmente, la falta de una decisión de adecuación podría desalentar la inversión extranjera, las empresas internacionales podrían ser reticentes a establecer operaciones en un país donde la protección

[14] El EEE se conforma por los países de la UE, más Liechtenstein, Islandia y Noruega.

de datos no es una prioridad, ya que podría dificultar sus relaciones comerciales transfronterizas.

Ante esta situación, la OCDE, el Convenio 108+ del Consejo Europeo y la Directiva 95/46/CE del Parlamento y del Consejo Europeo han establecido los cimientos que guían los principios regulatorios de esta materia. Actualmente, el Reglamento General de Protección de Datos de la UE se ha referido a las condiciones bajo las cuales es permitido llevar a cabo transferencias internacionales de datos personales con terceros países. Por ello, surge la siguiente pregunta de investigación:

¿Cuáles son los desafíos que Costa Rica debe enfrentar y las consideraciones normativas que deben existir para que la Unión Europea le conceda un nivel adecuado de protección de datos personales que simplifique la transferencia internacional de estos datos y convierta al país en un puerto seguro en pro de la facilitación comercial?

Preguntas secundarias

¿Cuál es el marco institucional costarricense e internacional existente en materia de transferencia internacional de datos personales?

¿Cuáles son las prácticas de la Unión Europea utilizadas para la transferencia internacional de datos personales y el proceso para otorgar una decisión de adecuación a un tercer país?

¿Cuáles son los desafíos existentes para que se dé una transferencia internacional de datos entre Costa Rica y la Unión Europea?

¿Cuáles son algunas recomendaciones para que Costa Rica logre una futura decisión de adecuación con la Unión Europea?

1.4. Objetivos

1.4.1. Objetivo General

Analizar los desafíos que Costa Rica debe enfrentar y las consideraciones normativas que deben existir para que la Unión Europea le conceda un nivel adecuado de protección de datos personales que lo convierta en un puerto seguro en pro de la facilitación comercial.

1.4.2. Objetivos Específicos

1. Describir el marco institucional internacional y costarricense existente en materia de transferencia internacional de datos personales, con el fin de comprender la situación normativa actual.

2. Examinar prácticas de la Unión Europea para la transferencia internacional de datos personales, para así reconocer el proceso que conlleva una decisión de adecuación.

3. Determinar desafíos normativos e institucionales existentes en Costa Rica para lograr una decisión de adecuación que le permita efectuar transferencias internacionales de datos personales con la Unión Europea.

CAPÍTULO II: MARCO CONCEPTUAL Y METODOLÓGICO

2.1. Marco conceptual

Al abordar el tema de la presente investigación es necesario considerar una serie de conceptos que permiten comprender de manera integral la transferencia internacional de datos personales y su vinculación con el comercio. En este sentido, se desarrollan los siguientes temas: a) la definición de datos personales, privacidad y consentimiento informado, b) la conceptualización de la transferencia internacional de datos personales, c) un acercamiento a los conceptos de decisión de adecuación y nivel de protección adecuado desde el régimen de la Unión Europea, y iv) el término de puerto seguro para la transferencia internacional de datos personales y la facilitación del comercio.

2.1.1. Definición de datos personales, privacidad y consentimiento informado

Ahora bien, en el marco de esta investigación resulta fundamental comprender el concepto de datos personales. Según la Comisión Europea (s.f.) los datos personales

> (...) son cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal. Los datos personales que hayan sido anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales (párr. 1-2).

Destacan como ejemplos de datos personales no sensibles: a) nombre y apellidos, b) domicilio, c) dirección de correo electrónico, d) número de documento nacional de identidad, e) datos de localización, f) dirección de protocolo de internet, g) el identificador de la publicidad del teléfono, etc (Comisión Europea, s.f.). Por otra parte, existe lo que se denomina como datos personales sensibles, para la Organización de los Estados Americanos (OEA, 2021) este término:

> (...) se refiere a una categoría más estrecha que abarca los datos que afectan a los aspectos más íntimos de las personas físicas… En ciertas circunstancias podría considerarse que estos datos merecen protección especial porque, si se manejan o divulgan de manera indebida, podrían conducir a graves perjuicios para la persona o a discriminación ilegítima o arbitraria (p. 24).

Dentro de los datos personales que se consideran sensibles se encuentran: a) los datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, b) la afiliación sindical, c) datos genéticos, datos biométricos tratados únicamente para identificar un ser humano, d) datos relativos a la salud, y e) datos relativos a la vida sexual u orientación sexual de una persona (Comisión Europea, s.f.). Estos datos se encuentran normados en el artículo 4 apartados 13, 14 y 15 y en el artículo 9 apartado 1 del Reglamento (UE) 2016/679, el cual establece la prohibición del tratamiento de esta categoría de datos sensibles; sin embargo, existen excepciones en esta jurisprudencia[15] en las que sí pueden tratarse; por ejemplo, si el interesado dio su consentimiento explícito o si el tratamiento es necesario para el cumplimiento de obligaciones o para proteger intereses vitales del interesado.

Cordero (2019) argumenta que "(...) dentro del amplio ámbito de la protección de datos las transferencias internacionales de datos personales tienen una importancia muy significativa por su incidencia en las operaciones transfronterizas" (p. 51). Cabe destacar que fuera del EEE existe jurisprudencia que puede considerarse poco exigente o incluso nula, al no existir reglamentación en la materia. Por lo que,

> La dispar reglamentación existente en este ámbito puede conducir en la práctica a que quede sin efectos la buscada protección de este tipo de datos por el Derecho europeo cuando aquellos se localicen en países con un nivel de protección inferior o simplemente inexistente (p. 52).

Por otra parte, es de vital relevancia para esta investigación analizar el término de la privacidad. De acuerdo con la OEA (2021) la privacidad "(...) se basa en los conceptos fundamentales del honor personal y la dignidad, así como en la libertad de expresión, pensamiento, opinión y asociación, reconocidos por los principales sistemas de derechos humanos del mundo" (p.21). A partir del auge de los mercados globales y de las tecnologías digitales, este concepto se ha transformado y actualmente "(...) se extiende a una amplia gama de datos personales e información que se puede almacenar en nuestros dispositivos digitales personales, en centros de datos corporativos e incluso en la nube" (IBM Security, 2019, p. 3).

Aunado a lo anterior, el consentimiento se caracteriza por ser un principio esencial en la protección de datos, ya que "permite que el interesado controle cuándo sus datos personales

[15] Artículo 9, apartado 2 del Reglamento (UE) 2016/679.

serán sometidos a un tratamiento" (Privacy International, s.f., p. 1). Esto implica que el consentimiento del individuo

> (...) debería basarse en suficiente información y debería ser claro, es decir, no debería dar lugar a ninguna duda o ambigüedad con respecto a la intención de la persona… La persona debería ser capaz de efectuar una elección real y no debería correr ningún riesgo de engaño, intimidación, coacción o consecuencias negativas significativas si se niega a dar el consentimiento (OEA, 2021, p. 32).

Es por esta razón, que en la actual era digital una adecuada protección de datos personales en terceros países es fundamental para cumplir con la reglamentación europea, siendo más importante aún el asegurarse que no exista ningún tipo de afectación hacia los derechos y la privacidad de las personas. Para el caso de esta investigación estos conceptos son clave pues implican que detrás del dato hay una persona, y por eso, es tan importante garantizar su integridad en los flujos transfronterizos de datos personales.

2.1.2. Conceptualización de la transferencia internacional de datos personales

Actualmente, gran cantidad de países alrededor del mundo regulan las transferencias transfronterizas de datos personales; no obstante, no existe a nivel mundial un instrumento jurídico integral que abarque a todos los Estados y se aplique de manera uniforme. Por tal razón, las regulaciones en esta materia difieren de país a país. De acuerdo con el Banco Mundial (2021), los países siguen tres enfoques generales:

a. Transferencias abiertas de datos: este modelo se caracteriza por la ausencia de restricciones gubernamentales, los países que lo aplican suelen darle a las empresas la libertad de autorregularse (confianza en las normas y prácticas del sector privado) y son en la mayoría de ocasiones las responsables del tratamiento de los datos personales que reciben. En este caso, el papel del gobierno es ejercer la responsabilidad ex-post al llevar a cabo acciones coercitivas, como multas. Este enfoque suscita una preocupación, ya que no garantiza ningún nivel mínimo de protección de los datos personales. Como ejemplo de este modelo sobresalen las Normas de Privacidad Transfronteriza adoptadas por la Cooperación Económica Asia-Pacífico[16] que en lugar de solicitar la aprobación previa de una autoridad de protección de datos para las transferencias, se basan en la

[16] Actualmente la APEC cuenta con 21 miembros: Australia, Brunei Darussalam, Canadá, Corea, Chile, China, Estados Unidos, Filipinas, Hong Kong, Indonesia, Japón, Malasia, México, Nueva Zelandia, Papúa Nueva Guinea, Perú, Rusia, Singapur, Taiwán, Tailandia y Vietnam.

autocertificación por parte de las organizaciones. Otro caso es el de Estados Unidos, que carece de un marco nacional de protección de datos y se apoya en la Comisión Federal de Comercio para supervisar el cumplimiento de las prácticas de protección de datos de las empresas privadas. Este modelo se ha adoptado por 39 de los 116 países encuestados para el Informe sobre el Desarrollo Mundial del 2021.

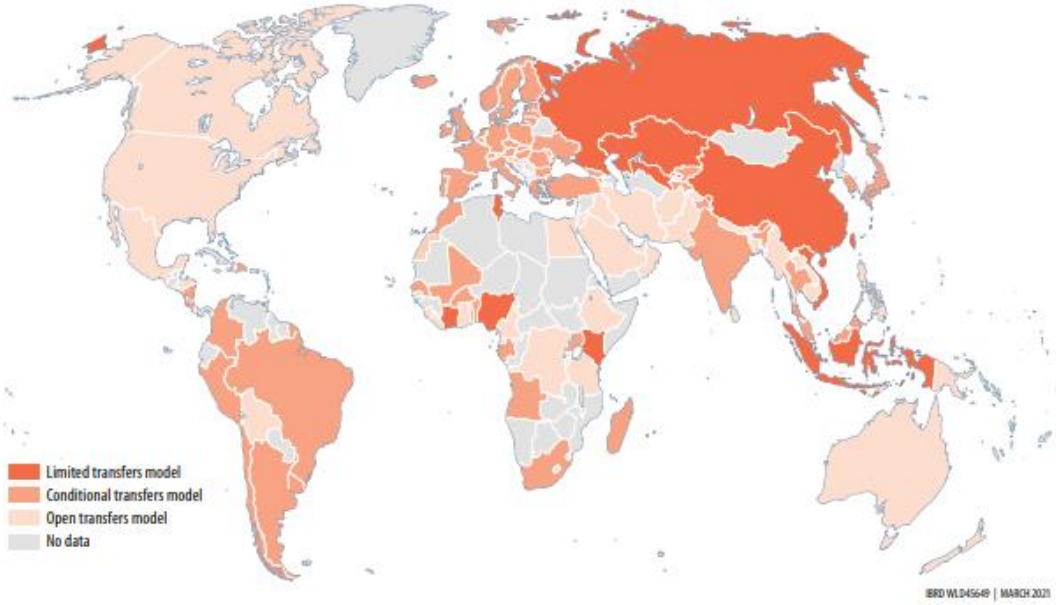
b. Transferencias condicionadas de datos: este modelo busca un equilibrio entre la protección de datos y la necesidad de que se efectúen las transferencias de datos. Por ello, establece salvaguardias reglamentarias obligatorias, una vez satisfechas, posibilitan la libre circulación de datos a nivel transfronterizo; sin embargo, si un país no cumple los requisitos, el intercambio de datos se ve restringido. Destaca la Unión Europea como un pionero en este tipo de modelo con la Directiva 95/46 y el posterior RGPD. Un enfoque similar ha sido adoptado por países como Argentina, Colombia, Corea del Sur, Senegal, Sudáfrica, etc. De acuerdo con el Informe sobre el Desarrollo Mundial del 2021, este modelo se ha adoptado por 66 de los 116 países encuestados.

c. Transferencias limitadas: este modelo cuenta con un enfoque más restrictivo de los flujos de datos transfronterizos, ya que se requiere la aprobación reglamentaria explícita de las transferencias internacionales de datos, en algunas ocasiones, puede requerir la localización de los datos y una autorización ex-ante del Gobierno. Frecuentemente, este modelo incluye la condición de almacenar y, en algunas ocasiones, procesar los datos personales dentro del país de origen. Un régimen de este tipo puede restringir enormemente los flujos de comercio digital. Por ejemplo, China demanda requisitos estrictos para las transferencias de datos personales; además, existen condiciones obligatorias para los datos denominados "infraestructura de información crítica" (información financiera, datos personales, datos médicos, etc.), los operadores de este tipo de información tienen la obligación de almacenar cierta información personal y empresarial en China. Otro caso es el de Rusia, dado a que su Ley de Datos Personales exige que todos los datos personales de los ciudadanos rusos se almacenen y procesen en bases de datos ubicados dentro del país. Este modelo se ha adoptado por 11 de los 116 países encuestados.

Tal y como afirma el Banco Mundial (2021), la variedad de modelos de regulación en los distintos países deja en evidencia que el "(...) comercio digital, y en particular la regulación de los flujos transfronterizos de datos ha pasado a ocupar un lugar en la agenda de la gobernanza

mundial"[17]. Esta diferencia evidencia cómo los objetivos de las políticas públicas de los diferentes países varían, unos abogan por la libertad de las empresas, otros por la protección de datos personales y otros por la seguridad nacional. Adicionalmente, "La gran variedad de enfoques existentes en todo el mundo pone de manifiesto las distintas prioridades políticas, así como la percepción de las oportunidades y los riesgos"[18] (p. 238). A continuación, se muestra la figura 2, que presenta los modelos de regulación de los flujos de datos transfronterizos a nivel mundial.

Figura 2. Modelos de regulación de los flujos de datos transfronterizos



Fuente: Tomado de Banco Mundial (2021)

En este sentido, es necesario definir qué se entiende por transferencia internacional de datos en el contexto del ordenamiento jurídico para así enmarcar el objeto de estudio y, consecuentemente poseer las herramientas necesarias que promuevan una mejor comprensión de los desafíos existentes con respecto a la protección efectiva de los datos personales de un tercer país, como lo es Costa Rica.

En cuanto al concepto de transferencia internacional de datos, Gonzalo (2019) lo define como "(...) aquellos datos personales se divulgan o se ponen a disposición de un receptor sujeto

[17] Traducción libre. Texto original: "Digital trade—and in particular the regulation of cross-border data flows—has risen rapidly on the global governance agenda".

[18] Traducción libre. Texto original: "The wide range of approaches across the globe highlights the various policy priorities as well as the perceptions of opportunities and risks".

a la jurisdicción de otro Estado u organización internacional" (p. 352). Por su parte, en el ordenamiento jurídico europeo actual no figura una definición explícita sobre la protección de datos en cuanto a la transferencia internacional a terceros países. En el artículo 4 apartado 23 del Reglamento (UE) 2016/679 se hace referencia al tratamiento transfronterizo de datos personales en los Estados miembros, pero no hacia terceros países; y en el Reglamento (UE) 2018/1725 en el artículo 3 no se incorpora ninguna definición. No obstante, la normativa española sí incorpora el concepto de transferencia internacional de datos en el artículo 5 apartado s del Real Decreto 1720/2007 de 21 de diciembre (RLOPD)[19] y lo define como el:

> Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español (p. 10).

De acuerdo con este concepto, se entiende que las transferencias internacionales son aquellas que implican un flujo de datos que se da desde España hacia países que se encuentran fuera del Espacio Económico Europeo (EEE).

> (...) aplicado al contexto del Reglamento supone que el flujo de datos tiene origen en un Estado del EEE y como destino un tercer Estado. Así, existirá transferencia internacional cuando ésta constituya una cesión o comunicación de datos o cuando tenga por objeto la realización de un tratamiento de datos por cuenta del responsable, produciéndose una salida física de datos fuera del EEE (Cordero, 2019, p. 57).

Esta conceptualización es relevante para la investigación porque proporciona una comprensión de los diversos modelos de regulación de los flujos transfronterizos de datos personales a nivel mundial, reflejando las prioridades de cada país. Además, al clasificar a la Unión Europea en la categoría de transferencias limitadas, ayuda a entender su posición con respecto a la protección de datos y sus implicaciones en el contexto internacional.

[19] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

2.1.3. Un acercamiento a los conceptos de decisión de adecuación y nivel de protección adecuado desde el régimen de la Unión Europea

El régimen de la UE en cuanto a las transferencias internacionales de datos personales hacia un tercer país u organizaciones internacionales proporciona varios instrumentos que posibilitan la circulación de los datos con un elevado nivel de protección. Por tanto, se abordará en este apartado el concepto de decisión de adecuación y, con este, el de nivel de protección adecuado.

Las transferencias basadas en una decisión de adecuación se encuentran normadas en el artículo 47 del Reglamento (UE) 2018/1725, en el inciso 1 se establece que podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión Europea haya decidido que:

> (...) el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado y cuando los datos se transfieran exclusivamente para permitir el ejercicio de funciones que sean competencia del responsable del tratamiento.
>
> Esto quiere decir que las decisiones de adecuación:
>
> (...) permiten la libre circulación de datos personales desde la UE sin que el exportador de datos de la Unión tenga que aportar ninguna garantía adicional ni cumplir otras condiciones… Por consiguiente, las transferencias al país interesado se asimilarán a las transmisiones de datos dentro de la Unión, lo que permitirá el acceso privilegiado de dicho país al mercado único europeo y la apertura de canales comerciales para los operadores de la UE (Comisión Europea, 2017, p. 7).

Lo anterior, significa que cuando la Comisión Europea le otorga una decisión de adecuación a un determinado país es porque cumple con ofrecer un nivel de protección adecuado que se asemeja al de la UE, esto no implica que la normativa del tercer país debe ser idéntica a la de la UE. Ahora la pregunta es: ¿qué significa contar con un nivel de protección adecuado? De acuerdo con el Grupo de Trabajo del artículo 29[20], en adelante GT29 (2018) indica que para considerar un nivel de protección adecuado, la Comisión tomará en cuenta "(...) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la

[20] El GT29 fue creado por la Directiva 95/46/CE y su función era tratar cuestiones relacionadas con la protección de la privacidad y los datos personales. El GT29 fue sustituido el 25 de mayo de 2018 por el Comité Europeo de Protección de Datos (CEPD) con la entrada en aplicación del RGPD.

legislación pertinente, la existencia y funcionamiento efectivo de una o más autoridades de control independientes y los compromisos internacionales que haya adoptado el tercer país" (p. 3).

Por consiguiente, resulta evidente que cualquier evaluación de la protección adecuada debe comprender dos aspectos esenciales, el contenido de las normas que son aplicables y los medios que garantizarán su aplicación. Adicionalmente, la Comisión tiene la responsabilidad de verificar periódicamente (al menos cada cuatro años) que lo acordado en la decisión de adecuación continúe siendo efectivo a nivel práctico (GT29, 2018).

Este acercamiento inicial a los conceptos de decisión de adecuación y nivel de protección adecuado es clave para comprender el propósito de la presente investigación, ya que si Costa Rica aspira a contar con una libre circulación de datos personales con la UE debe obtener una decisión de adecuación que lo faculte. El capítulo IV profundiza en estos términos.

2.1.4. El término de puerto seguro para la transferencia internacional de datos personales y la facilitación del comercio

El término de puerto seguro suele asociarse con el acuerdo entre Estados Unidos y la UE, denominado *Safe Harbor* o puerto seguro del año 2000. Adicionalmente, no se encuentra en la literatura una definición de este término que no se vincule con el acuerdo citado. Por ello, para los fines de esta investigación, se entenderá puerto seguro como un país o una región que proporciona un nivel adecuado de protección de datos al realizar transferencias internacionales de datos personales; asimismo, un puerto seguro no sólo se limita a la protección de datos en tránsito, sino que también implica un uso y una protección apropiada una vez que llegan a su destino. En este sentido, la Comisión Europea indica que:

> El respeto de la privacidad constituye un requisito para garantizar la estabilidad, seguridad y competitividad de los flujos comerciales mundiales. La privacidad no es un producto con el que se pueda negociar. Internet y la digitalización de bienes y servicios han transformado la economía mundial, y la transferencia transfronteriza de datos, incluidos los de carácter personal, figura entre las actividades cotidianas de las empresas europeas de todos los tamaños y ámbitos. Puesto que los intercambios comerciales dependen cada vez más de la circulación de datos personales, la protección y seguridad de estos últimos se ha convertido en un factor fundamental de la confianza de los consumidores (p. 6).

Hoy en día, y más que nunca, los intercambios globales de bienes y servicios son sustentados por los flujos transfronterizos de datos. De acuerdo con la Organización para la Cooperación y el Desarrollo Económicos, OECD (2022) "Estos flujos permiten que las empresas creen y gestionen complejas cadenas de suministro mundiales, que las organizaciones compartan datos para la investigación y que los consumidores busquen información sobre bienes y servicios ofrecidos en todo el mundo" (p. 12). Es así como la circulación de datos facilita el comercio al impulsar las operaciones comerciales y la provisión de servicios; y además, fortalece la colaboración entre empresas y países a nivel internacional.

Ante el crecimiento constante de la digitalización y la interconexión global, la protección de datos se convierte en una prioridad ética y práctica tanto para las empresas como para los países que buscan participar en los flujos comerciales globales de manera segura y responsable. Al respecto, la OMC (2018) indica que "La ausencia de leyes de protección de datos puede mermar la confianza en numerosas actividades comerciales" (p. 157). Por lo tanto, es crucial mantener la confianza de los interesados (consumidores, empresas, países) para asegurar la continuidad de los intercambios comerciales.

2.2. Marco metodológico

En esta sección se presenta la metodología empleada para lograr los objetivos de la investigación, esto implica la explicación del método de investigación, los sujetos de investigación, la descripción de las técnicas e instrumentos por objetivos, las fuentes de información y los alcances y limitaciones.

2.2.1. Método de la investigación

Debido a que el tema de esta investigación es poco explorado y existe muy poca evidencia, el enfoque de la presente investigación es de carácter cualitativo. Según Sampieri (2018) este se basa en "(...) una lógica y proceso inductivo (explorar y describir, y luego generar perspectivas teóricas)" (p. 8). Por ello este tipo de investigación, se caracteriza por no ser lineal, lo que significa, que las etapas de la investigación no son secuenciales; por el contrario "la acción indagatoria se mueve de manera dinámica en ambos sentidos: entre los hechos y su interpretación, y resulta un proceso más bien circular en el que la secuencia no siempre es la misma, pues varía con cada estudio" (Sampieri, 2018, p. 7).

Ahora bien, el tipo de diseño de investigación es exploratorio, dadas las especificidades del tema y la poca investigación en esta área. De acuerdo con Sampieri (2018), los estudios

exploratorios se efectúan cuando "(…) el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes". Además "(…) en pocas ocasiones constituyen un fin en sí mismos. Generalmente determinan tendencias, identifican áreas, ambientes, contextos y situaciones de estudio, relaciones potenciales entre variables…" (p. 91).

A partir de la investigación, se pretende realizar un análisis que le añada valor a la investigación y a Costa Rica en el ámbito de la transferencia internacional de datos personales, al ser un tema poco estudiado, ya que se busca identificar los desafíos existentes para que el país se considere un puente seguro y pueda efectuar transferencias internacionales de datos personales con la Unión Europea. Adicionalmente, se determinará si este flujo de datos es clave para el desarrollo del país en términos de comercio, cooperación y transparencia, y si una adecuación del Consejo Europeo beneficiaría a Costa Rica. Seguidamente, se detallan los sujetos de investigación.

2.2.2. Sujetos de investigación

Tal y como afirma Sampieri (2018) "En ciertos estudios es necesaria la opinión de expertos en un tema. Estas muestras son frecuentes en estudios cualitativos y exploratorios para generar hipótesis más precisas" (p. 387). Por tal motivo, se seleccionaron como sujetos de investigación a personas con conocimiento y experiencia en lo referente a la transferencia internacional de datos personales con el fin de obtener una comprensión de los diversos aspectos relacionados con la transferencia internacional de datos personales, para la identificación de desafíos y de futuros escenarios en la materia. Las personas entrevistadas fueron las siguientes:

a. Mauricio Garro Guillén: consultor jurídico experto en protección de datos personales y profesor universitario.
b. Jostin Durán Durán: administrador público y asesor profesional en la Asamblea Legislativa.
c. Persona entrevistada: funcionario del Ministerio de Comercio Exterior (COMEX).
d. Alejandro Ross Muñoz: analista de privacidad.
e. Roberto Lemaitre Picado: ingeniero informático, abogado especialista en ciberseguridad y derecho digital, y profesor universitario.

2.2.3. Descripción de las técnicas e instrumentos de recolección

Análisis documental

Los documentos, materiales y registros facilitan la comprensión del fenómeno central de estudio. Sampieri señala que estas fuentes "(...) le sirven al investigador para conocer los antecedentes de un ambiente, así como las vivencias o situaciones que se producen en él" (p. 415). A través del análisis documental, se describió el marco institucional internacional y nacional en lo concerniente a la transferencia internacional de datos personales (objetivo específico 1), para lo cual se realizaron las siguientes actividades:

a. Se llevó a cabo una búsqueda e identificación del marco institucional internacional y nacional referente a la transferencia internacional de datos personales a través de sitios de internet de los gobiernos y de organizaciones que se encuentran vinculadas al tema en estudio como la Comisión Europea, el Consejo de Europa, el GT29 y la OECD.

b. Posteriormente, se clasificaron los documentos en dos categorías: marco institucional internacional y marco institucional nacional. Para esto, se elaboró la tabla 1 y 2, en las que se clasificaron los documentos encontrados.

c. Por último, se efectuó un análisis de lo encontrado, esto permitió una comprensión de la situación normativa actual a nivel nacional e internacional con respecto a la transferencia internacional de datos personales.

Para el análisis de estos documentos se exploraron los siguientes temas que orientaron el análisis de contenido: el fin de la normativa, la vinculación con la protección de datos personales en los flujos transfronterizos y la existencia de una agencia de protección de datos.

Tabla 1. Documentos consultados sobre el marco institucional internacional en materia transferencia y protección de datos personales

Año de publicación	Gobierno u organización	Nombre del documento
2002	OCDE	Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales
1981	Consejo de Europa	Convenio 108
2018	Consejo de Europa	Convenio 108+
2018	Parlamento Europeo y	Reglamento General de Protección de datos

	Consejo de Europa	(RGPD): decisión de adecuación con Japón, Reino Unido y Estados Unidos
2017	Red Iberoamericana de Protección de Datos	Estándares de Protección de Datos de los Estados Iberoamericanos
1853, 2000, 2016	Congreso de la Nación de Argentina	Constitución Nacional, Ley de Protección de Datos Personales, Ley de Acceso a la Información Pública
2008	Parlamento del Uruguay	Ley de Protección de Datos Personales

Fuente: elaboración propia

Tabla 2. Documentos consultados sobre el marco institucional nacional en materia transferencia y protección de datos personales

Año de publicación	Gobierno u organización	Nombre del documento
2011	Asamblea Legislativa de Costa Rica	Ley de Protección de la Persona frente al tratamiento de sus datos personales No. 8968 y su Reglamento
2021	OCDE	Recomendaciones de la OCDE para Costa Rica
2022	Asamblea Legislativa de Costa Rica: Eliécer Feinzaig Mintz y otros diputados	Proyecto de Ley No. 23097: Ley de Protección de Datos Personales

Fuente: elaboración propia

Además, mediante el análisis documental se examinaron prácticas de la Unión Europea para la transferencia internacional de datos personales y el proceso que conlleva una decisión de adecuación (objetivo específico 2). Para esto se elaboró la tabla 3, en la cual se sintetizan los documentos consultados. Se investigaron los siguientes temas para guiar el análisis de contenido de estos documentos: los criterios para determinar una decisión de adecuación y su proceso y los mecanismos alternativos para la transferencia de datos personales.

Tabla 3. Documentos consultados sobre las prácticas de la Unión Europea para la transferencia internacional de datos y las decisiones de adecuación

Año de publicación	Organización o autor(a)	Nombre del documento
2017	Comisión Europea	Comunicación de la Comisión al Parlamento Europeo y al Consejo: Intercambio y protección de los datos personales en un mundo globalizado.
2018	GT29	Referencias sobre adecuación

2019	Clara Isabel Cordero Álvarez	La transferencia internacional de datos con terceros Estados en el nuevo Reglamento Europeo
2021	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)	Nuevo régimen europeo de protección de datos personales: la adecuación de tercer país
2021	Andoni Polo Roca	Las transferencias internacionales de datos: regulación actual y su incidencia en las relaciones exteriores de la Unión Europea
2023	Mariana Patricia Fantini	Transferencia internacional de datos: ¿por qué desafiar el statu quo de la normativa local argentina? Un análisis a partir del marco regulatorio de la Unión Europea

Fuente: elaboración propia

Entrevistas

Para Sampieri (2018) se puede definir la entrevista como:

> (...) una reunión para conversar e intercambiar información entre una persona (el entrevistador) y otra (el entrevistado) u otras (entrevistados)... En la entrevista, a través de las preguntas y respuestas se logra una comunicación y la construcción conjunta de significados respecto a un tema (p. 403).

La realización de entrevistas en esta investigación estuvo dirigida a personas con conocimiento y experiencia en materia de protección y transferencia internacional de datos personales. Las cinco personas que se entrevistaron fueron elegidas a conveniencia por su conocimiento y experiencia en el ámbito de estudio. Para la entrevista se elaboró un cuestionario de entrevista (ver anexo 1) conformada por diez preguntas abiertas, ya que se buscaba recabar información específica sobre la perspectiva de los expertos en la materia. Los temas que se abordaron fueron los siguientes:

a. Conocimiento general sobre la transferencia internacional de datos personales.
b. Costa Rica: situación actual y consideraciones normativas sobre la transferencia internacional de datos personales.
c. Unión Europea: legislación y prácticas relacionadas con la transferencia internacional de datos personales.
d. Desafíos normativos e institucionales para Costa Rica y perspectivas futuras.

El análisis de las respuestas fue efectuado de forma manual al ser pocos sujetos de investigación. Para ello, se revisó cada respuesta individualmente, de esta forma se encontraron similitudes y diferencias entre ellas. A partir de la recolección de la información y su sistematización se elaboraron tablas e infografías que permitieron analizar la información y obtener una mejor comprensión de los resultados.

Estas entrevistas, contribuyeron con el objetivo específico 1 al brindar una mayor comprensión sobre los principales motivos para la transferencia internacional de datos personales. También, con el objetivo específico 2, ya que se recabó información sobre la Unión Europea y la influencia que ha tenido el RGPD a nivel mundial. Adicionalmente, proporcionó información para contestar el objetivo específico 3, que tiene que ver con la determinación de desafíos existentes en Costa Rica para lograr una decisión de adecuación que le permita efectuar transferencias internacionales de datos personales con la Unión Europea.

2.2.4. Fuentes de información

Fuentes primarias

a. Normativa nacional e internacional: al ser documentos legales oficiales emitidos por autoridades legislativas y gubernamentales.

b. Entrevistas: implican la obtención de información directamente de una persona con conocimiento o experiencia relevante sobre el tema en cuestión.

Fuentes secundarias

a. Artículos científicos: sintetizan información existente, revisan literatura previa o proporcionan una interpretación y análisis de datos ya publicados.

b. Tesis: promueven el debate y la discusión sobre un tema importante, sensibilizan sobre un problema o una necesidad. Revisan literatura previa, recopilan datos y recomiendan soluciones a un problema.

2.2.5. Alcance y limitaciones

La investigación se enfocó en el análisis de las condiciones que deben existir para que la Unión Europea le conceda a Costa Rica un nivel adecuado de protección de datos personales que facilite la transferencia internacional de datos, convierta a Costa Rica en un puerto seguro y facilite el comercio. Dentro de las limitaciones de la investigación se pueden mencionar:

a. La falta de literatura específica para Costa Rica sobre las transferencias internacionales de datos personales.

b. El número limitado de entrevistas realizadas, una mayor cantidad de entrevistas hubiera proporcionado una visión más amplia. Además, se intentó programar una entrevista con la Delegación de la Unión Europea en Costa Rica, pero no hubo una respuesta positiva.

c. La carencia de estadísticas que muestren la contribución de los flujos de datos transfronterizos a los intercambios comerciales.

Capítulo III: Marco institucional internacional y nacional en materia del flujo transfronterizo de datos personales

En este capítulo se abordará el marco institucional internacional y nacional en lo referente a la transferencia internacional de datos personales con el fin de comprender la situación normativa actual. Para lograr este objetivo, se realizó una revisión documental. En este sentido, el capítulo se estructura de la siguiente manera: a) preámbulo sobre el intercambio comercial Unión Europea-Costa Rica, b) marco institucional internacional: Directrices de la OCDE, Convenio 108 y 108+, el RGPD y algunos ejemplos de decisiones de adecuación, Estándares de Protección de Datos de los Estados Iberoamericanos, y la normativa de dos países Latinoamericanos, Argentina y Uruguay; y c) marco institucional nacional: Ley de Protección de la Persona frente al tratamiento de sus datos personales, el Proyecto de Ley No. 23.097 y las recomendaciones de la OCDE para Costa Rica.

3.1. Preámbulo sobre el intercambio comercial Unión Europea-Costa Rica

En mayo de 2010, seis países centroamericanos (Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá) concluyeron las negociaciones del Acuerdo de Asociación entre la Unión Europea y Centroamérica (AACUE). Este acuerdo abarca tres pilares: comercio, diálogo político y cooperación; el primero entró en vigencia en Costa Rica el 1 de octubre de 2013. La UE, alcanzó una liberalización inmediata del 69% de sus exportaciones a Centroamérica (CA), el restante será liberalizado en un máximo de 15 años. Por otra parte, CA consiguió un acceso libre para los productos industriales a la UE desde que entró en vigor el AACUE; adicionalmente, se concertaron calendarios para la liberalización completa de otros productos, exceptuando la leche en polvo y el queso. Otro de los objetivos del AACUE consiste en fomentar la integración económica de la región centroamericana (Oficina Económica y Comercial de España en Panamá, 2022).

Con respecto a los intercambios comerciales, la UE destaca como un importante socio para Costa Rica, de acuerdo con Oficina Económica y Comercial de España en Panamá (2022):

> (...) las importaciones con origen Costa Rica vienen manteniendo un peso de aproximadamente un 43% del total de las importaciones de la UE provenientes de Centroamérica en los últimos cinco años, siendo por tanto, y con diferencia, el primer proveedor centroamericano de la UE (p. 40).

Las exportaciones de Costa Rica hacia la UE alcanzaron un valor de €4.531 millones en 2023, la tasa de crecimiento de las exportaciones de Costa Rica tomando como referencia el año 2012 es de un 206%[21]. Los países de la UE a los cuáles se destina la mayor parte de las exportaciones de Costa Rica son Países Bajos, Bélgica y España. Los principales productos importados por la UE son dispositivos médicos, banano, piña, circuitos integrados, microestructuras electrónicas, café, etc.

Por otra parte, las exportaciones de la UE hacia Costa Rica sumaron €1.705 millones en 2023, lo que representa un incremento de un 148% con respecto al 2012[22]. Los países de la UE de los cuáles provienen la mayor cantidad de bienes importados por Costa Rica son Alemania, España e Italia. Los principales productos importados por Costa Rica son vehículos, productos farmacéuticos, máquinas y aparatos médicos, aceites de petróleo, entre otros.

3.2. La motivación de los países y empresas para llevar a cabo el flujo transfronterizo de datos personales

El flujo transfronterizo de datos personales se ha convertido en una necesidad imperante tanto para los países como para las empresas en la era digital actual. Al respecto, Garro (comunicación personal, 7 de febrero de 2024) afirma que:

> (...) la transferencia de datos cobra un especial realce sobre todo a finales de los 90 y a principios de los 2000 cuando se produce la explosión de las redes sociales, con el origen del big data y paralelamente con el surgimiento de las tecnologías más avanzadas, el machine learning en la inteligencia artificial y los productos derivados del tratamiento de datos con algoritmos.

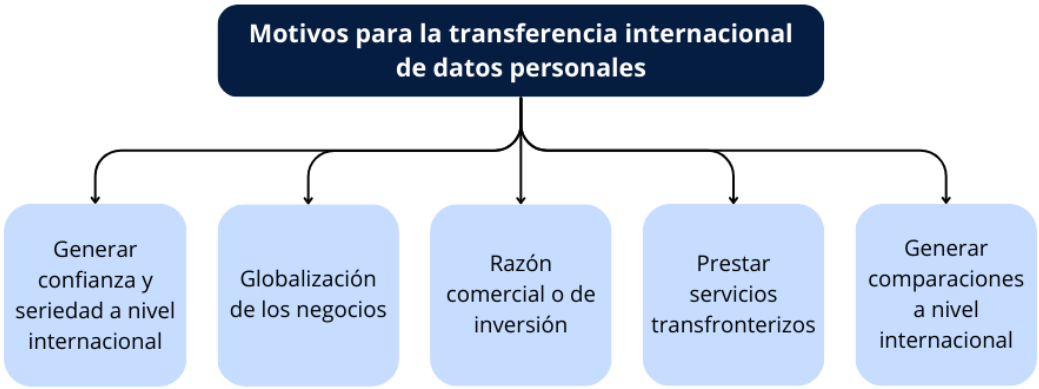
En este sentido, existen una variedad de motivos por parte de los países y de las empresas para propiciar el intercambio de datos personales. De las entrevistas realizadas, se extraen las principales razones para la transferencia internacional de datos personales: a) generar confianza y seriedad a nivel internacional sobre cómo el país o los países toman la protección de datos de sus ciudadanos, b) la globalización de los negocios debido a que el alcance de las empresas en esta era digital puede ser global, c) una razón comercial o de

[21] Las exportaciones de Costa Rica hacia la UE en 2012 fueron de €1.480 millones. Los datos se toman de Access2Markets.

[22] Las exportaciones de la UE hacia Costa Rica en 2012 fueron de €688 millones. Los datos se toman de Access2Markets.

inversión, d) prestar servicios transfronterizos para generar comercio y e) generar comparaciones a nivel internacional que le permita a los países generar política pública. La figura 3 sintetiza lo expuesto anteriormente:

Figura 3. Principales motivos para la transferencia internacional de datos personales



Fuente: elaboración propia con información tomada de las entrevistas realizadas.

Estos intercambios de datos son impulsados por la necesidad de adaptarse a un entorno globalizado y generar oportunidades comerciales y de desarrollo a nivel internacional. Garro señala la importancia de los flujos transfronterizos de datos al afirmar que "(...) sin esa transferencia, sin esos movimientos, no existiría la evolución de los mercados modernos y de las sociedades como las conocemos en el mundo occidental".

3.3. Marco institucional internacional en materia del flujo transfronterizo de datos personales

Comprender el marco institucional internacional en lo referente al flujo transfronterizo de datos personales resulta pertinente para los fines de esta investigación. En este contexto, diversos acuerdos, estándares, directrices y marcos legales se han establecido a nivel internacional para abordar esta temática, con el objetivo de garantizar estándares de protección de datos personales en un entorno global; los cuales se explican a continuación.

3.3.1. Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE)

A partir de la incursión de la tecnología de la información en varias áreas de la vida económica y social y considerando la relevancia del procesamiento de datos mediante sistemas informáticos, la OCDE estableció en 1980 pautas concernientes a la protección de la privacidad y a los flujos transfronterizos de datos personales. Actualmente, el acelerado desarrollo de tecnologías de información y comunicación ha impulsado una rápida transición hacia una

sociedad global conectada basada en la información. A continuación, se muestra una figura que resume la evolución de las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales.

Figura 4. Evolución de las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales

Fuente: elaboración propia con información tomada de la OCDE (2002).

Estas directrices se dividen en cinco partes:

a. Generalidades: incluye definiciones importantes como controlador de datos, datos personales y flujo transfronterizo de datos personales. Adicionalmente, contempla el alcance de las directrices, donde se menciona que aplican a datos personales del sector público o privado (pp. 4-5).

b. Principios básicos de aplicación nacional: limitación de recogida, calidad de los datos, especificación del propósito, limitación de uso, salvaguardia de la seguridad, transparencia, participación individual y responsabilidad (pp.6-7).

c. Principios básicos de aplicación internacional: los países miembros deberán evitar la elaboración de marcos institucionales que pudieran crear obstáculos al flujo transfronterizo de datos personales (p. 8).

d. Implantación nacional: los países miembros deberán crear procedimientos o instituciones legales, administrativos o de otro tipo para garantizar la protección de la privacidad y las libertades individuales en relación con los datos personales (p. 9).

e. Cooperación internacional: los países miembros deberán establecer procedimientos para facilitar el intercambio de información relacionada con estas directrices y la cooperación en cuestiones procesales y de investigación (p.10).

3.3.2. Convenio 108 y 108+

El Convenio 108+ es una extensión del Convenio 108 del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, el cual constituye el primer instrumento internacional jurídicamente vinculante adoptado en la esfera de la protección de datos por más de 40 países europeos. La necesidad de modernización del Convenio surge a partir de las nuevas amenazas hacia los derechos humanos, particularmente contra el derecho a la vida privada. Lo anterior, emana del avance de nuevas tecnologías, de la globalización en el manejo de datos personales y del crecimiento exponencial del flujo de la información. Adicionalmente, el Convenio 108+ busca reforzar los mecanismos de evaluación y de seguimiento de este. (Parlamento Europeo, 2023). Es así como los principales cambios del Convenio se muestran en la tabla 4:

Tabla 4. Principales cambios contenidos en el Convenio 108+

Artículo	Convenio 108 de 1981	Convenio 108+ de 2018
Art. 1: objetivo y propósito	"El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»)".	"El presente Convenio tiene por objeto proteger a toda persona, sea cual fuere su nacionalidad o residencia, en lo que respecta al tratamiento de sus datos personales, contribuyendo al respeto de sus derechos humanos y libertades fundamentales, en particular el derecho a la privacidad". Con este planteamiento, el Convenio resalta cómo el tratamiento de datos personales puede permitir y promover el ejercicio de otros derechos esenciales.
Art. 2: definiciones	Incluye las definiciones de: datos de carácter personal, fichero automatizado, tratamiento automatizado, autoridad controladora de fichero.	Si bien no se modifican nociones esenciales como la definición de datos personales y la de interesados, se proponen otros cambios en las definiciones: se abandona el concepto de fichero, se sustituye la definición de responsable del fichero por responsable del tratamiento; además se adicionan los términos encargado del tratamiento y destinatario. Por otra parte, se incluye tanto el tratamiento automatizado como el no automatizado de datos personales que sea de la competencia de las Partes del Convenio.
Art. 5:	"Los datos de carácter personal que sean objeto de	Aclara la aplicación del principio de

calidad de los datos	un tratamiento automatizado: a) se obtendrán y tratarán legítimamente, b) se registrarán para finalidades determinadas, c) serán adecuados, pertinentes y no excesivos, d) serán exactos, y e) se conservarán de forma que permita la identificación de las personas durante un período de tiempo".	proporcionalidad para subrayar que debe aplicarse a lo largo de todo el tratamiento. Adicionalmente, se introduce una nueva disposición para establecer la base jurídica del tratamiento: el consentimiento (que para ser válido debe cumplir varios criterios) del interesado u otra base legítima establecida por la ley (contrato, interés vital del interesado, obligación legal del responsable del tratamiento, etc.).
Art. 6: categorías particulares de datos	"Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas".	El listado de datos sensibles se amplió a los datos genéticos y biométricos, así como los datos tratados por la información que revelan en relación con la afiliación sindical o el origen étnico.
Art. 7: seguridad de los datos	En el Convenio 108, únicamente se menciona que se tomarán medidas de seguridad apropiadas para proteger los datos de carácter personal.	En cuanto a la seguridad de los datos, se introduce la obligación de notificar sin demora cualquier violación de la seguridad.
Art. 8: transpa-rencia en el tratamiento	No se incluía en el Convenio 108.	Los responsables del tratamiento tendrán la obligación de garantizar la transparencia del tratamiento de los datos y, a tal fin, deberán facilitar una serie de informaciones requeridas, en particular relativas a su identidad y lugar habitual de residencia o establecimiento, sobre la base jurídica y los fines del tratamiento, los destinatarios de los datos y sobre las categorías de datos personales tratados. Además, deberán facilitar toda la información adicional necesaria para garantizar un tratamiento leal y transparente.
Art. 9: derechos del titular	En el Convenio 108, el artículo 8, garantías complementarias para la persona concernida estipulaba que cualquier persona deberá poder: a) conocer la existencia de un fichero automatizado	Se conceden nuevos derechos a los interesados para que tengan un mayor control sobre sus datos en la era digital. Por ejemplo, los interesados ahora tienen derecho a conocer el fundamento detrás del tratamiento de sus datos. Adicionalmente, los interesados tienen derecho a no ser objeto de una decisión que los afecte y que se base únicamente en el tratamiento automatizado, sin tener en cuenta la opinión del interesado. Por otra parte, tienen derecho a oponerse en cualquier momento al tratamiento de sus datos personales, a menos que el responsable del tratamiento demuestre motivos legítimos para el tratamiento que prevalezcan sobre sus intereses o derechos y libertades fundamentales.
Art. 14: flujos transfronte-	En el Convenio 108, las disposiciones no mencionan qué sucede si la transferencia se efectúa hacia un país que no se encuentra suscrito	La finalidad del régimen de flujo transfronterizo es garantizar que la información tratada originalmente en la jurisdicción de una Parte siga

rizos de datos personales	a la Convención, tampoco hace énfasis en cómo se asegura un nivel adecuado de protección de datos.	estando protegida por los principios adecuados de protección de datos. principios de protección de datos adecuados. En cuanto a los flujos transfronterizos de datos hacia un destinatario que no esté sujeto a la jurisdicción de una Parte, deberá garantizarse un nivel adecuado de protección en el Estado u organización receptores.

Fuente: elaboración propia con información del Consejo de Europa.

El Convenio 108+ es un instrumento que establece principios y valores para proteger a las personas, y simultáneamente funciona como un marco para el flujo transfronterizo de datos personales. Esto es relevante ya que la circulación internacional de información es cada vez más importante; sin embargo, esta transferencia debe respetar las libertades y los derechos de las personas. Asimismo, el desarrollo de nuevas tecnologías también debe estar acorde con estos derechos. Actualmente, los únicos países de Latinoamérica que forman parte del Convenio son Argentina, México y Uruguay (Consejo de Europa, 2019).

3.3.3. Un acercamiento al Reglamento General de Protección de Datos

El Reglamento General de Protección de datos (RGPD)[23] entró en vigor el 25 de mayo de 2018. De acuerdo con el Parlamento Europeo (2023) su fin es:

> (...) proteger a todos los ciudadanos de la Unión frente a las violaciones de la privacidad y de los datos personales en un mundo cada vez más basado en los datos, creando al mismo tiempo un marco más claro y coherente para las empresas (p. 3).

Esta norma tiene un papel fundamental en el marco de la Unión Europea para asegurar el derecho esencial a la protección de datos contenido en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea[24]. Adicionalmente, la Comisión Europea (2020) señala que:

[23] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

[24] Protección de datos de carácter personal: 1) Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan, 2) Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación, y 3) El respeto de estas normas quedará sujeto al control de una autoridad independiente.

> El RGPD ha reforzado las salvaguardias de protección de datos, aporta a los particulares derechos adicionales y más sólidos, una mayor transparencia, y garantiza que todos aquellos que tratan datos personales en el ámbito de su aplicación deban rendir más cuentas y tengan una mayor responsabilidad (p. 1).

En cuanto a la transferencia internacional de datos, en el considerando 101 del RGPD se resalta la importancia de estos flujos para la expansión del comercio y la cooperación. Adicionalmente, establece que si la transferencia se realiza a terceros países no se debe aceptar un nivel menor de protección al garantizado por el Reglamento.

Por otra parte, el capítulo 5 del RGPD hace referencia a la transferencia de datos personales a terceros países u organizaciones internacionales. En el artículo 45 indica que se podrá dar el flujo de datos transfronterizos cuando la Comisión haya decidido que el tercer país o la organización internacional garantizan un nivel de protección adecuado, para lo cual se tienen en cuenta los siguientes factores:

a. La efectividad del Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, las normas de protección de datos y las medidas de seguridad.

b. La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos.

c. Los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes en relación con la protección de los datos personales.

Es así como el RGPD proporciona un instrumento actualizado que facilita el flujo transfronterizo de datos personales, al mismo tiempo en que asegura que los datos sigan ostentando un nivel de protección elevado. Por ello, "(...) la Comisión ha intensificado su trabajo para aprovechar plenamente el potencial de los instrumentos disponibles en el marco del RGPD". Como parte de sus esfuerzos, se ha gestado una colaboración con partes que son clave, con el objetivo de lograr una decisión de adecuación, que permita "(...) la circulación segura y libre de datos personales al tercer país de que se trate sin necesidad de que el exportador de datos ofrezca más garantías u obtenga una autorización" (Comisión Europea,

2020, p. 13). Seguidamente, se analizarán tres decisiones de adecuación con el propósito de comprender los factores que llevan a estos países a lograr una decisión de adecuación por parte de la UE.

Decisión de adecuación mutua Unión Europea-Japón: la mayor zona mundial de circulación libre de datos con un elevado nivel de protección

En enero de 2019, la Comisión Europea adoptó la primera decisión de adecuación relativa a Japón conforme a lo expuesto en el artículo 45 del RGPD, en donde se concluía que este país "(…) garantiza un nivel de protección adecuado para los datos personales transferidos desde la Unión Europea a actividades económicas que manejan información personal situadas en Japón. Como consecuencia, pueden realizarse transferencias de datos desde la UE a operadores privados de Japón sin requisitos adicionales" (Comisión Europea, 2023, p. 1). La decisión de adecuación contempló:

a. La Ley sobre la Protección de la Información Personal de Japón (LPIP) es conocida como *Joho-Kakuho Hogo Ho* en japonés, fue promulgada en 2003 y modificada en 2015. Esta se creó con el fin de salvaguardar la información personal y su modificación reforzó las salvaguardas ya existentes e introdujo nuevas[25], logrando acercar este sistema de protección de datos al europeo.

b. Las reglas complementarias para salvar diferencias existentes entre la LPIP y el RGPD[26], las cuales refuerzan la protección de datos sensibles, los derechos individuales y las condiciones para efectuar una transferencia posterior de datos de la UE desde Japón hacia otro tercer país. Estas reglas "(…) son vinculantes para los operadores japoneses y son ejecutables por la autoridad independiente de protección de datos, es decir, la Comisión de Protección de la Información Personal (CPIP), o bien directamente por los particulares de la UE ante los tribunales japoneses" (Comisión Europea, 2023, pp. 1-2).

c. Las declaraciones, garantías y compromisos referentes a las limitaciones y salvaguardias con respecto al acceso y uso de los datos personales por parte de las

[25] Por ejemplo, se incluyen derechos individuales exigibles y el establecimiento de una unidad de control independiente, encargada de la supervisión y del control en la aplicación del LPIP.

[26] Véase el considerando 15 y el anexo 1 de la decisión de adecuación UE-Japón.

autoridades públicas japonesas, limitando el tratamiento a lo necesario y manteniéndolo bajo supervisión.

Cabe destacar que cuando se adoptó la decisión de adecuación, se creó "(…) la mayor zona mundial de circulación libre de datos basada en un elevado nivel de protección de datos" (Comisión Europea, 2023, p. 2). Lo anterior, ha promovido intercambios comerciales y creado oportunidades empresariales, lo cual muestra que "(…) en la era digital, la promoción de normas estrictas de protección de la intimidad y la facilitación del comercio internacional pueden y deben ir de la mano" (p. 2). En este sentido, los sistemas de Japón y de la UE han convergido, lo cual ha intensificado su cooperación en aspectos digitales, especialmente en lo referente al flujo de datos.

Decisión de adecuación Unión Europea-Reino Unido: tras el Brexit

La Comisión Europea adoptó en junio de 2021 dos decisiones de adecuación con respecto a las transferencias de datos personales al Reino Unido: a) la primera concerniente al RGPD y b) la segunda al amparo de la Directiva sobre protección de datos en el ámbito penal. Ante esto, el comisario de Justicia de la UE, Didier Reynders señaló que "Un flujo de datos seguros entre la UE y el Reino Unido es crucial para mantener estrechos lazos comerciales y cooperar eficazmente en la lucha contra la delincuencia." (Comisión Europea, 2021, p.1).

Dentro del marco de protección de datos del Reino Unido considerado para conceder la adecuación destaca la Ley de Retirada de la Unión Europea de 2018, *European Union (Withdrawal) Act*[27], antes de su retiro y durante su período de transición, la legislación sobre datos personales del Reino Unido era la aplicable a la UE, especialmente el RGPD. Ahora bien, de acuerdo con la Ley de Retirada "los tribunales del Reino Unido debían interpretar el Derecho de la Unión conservado no modificado de conformidad con la jurisprudencia pertinente del Tribunal de Justicia de la Unión Europea y los principios generales del Derecho de la Unión" (Comisión Europea, 2021, considerando 13).

Adicionalmente, los ministros del Reino Unido tienen la facultad de incluir legislación secundaria a través de instrumentos jurídicos para así llevar a cabo modificaciones en el Derecho de la Unión. Por ello, el marco normativo sobre la protección de datos en el Reino Unido consiste en: a) el RGPD del Reino Unido y el *Data Protection Act* de 2018

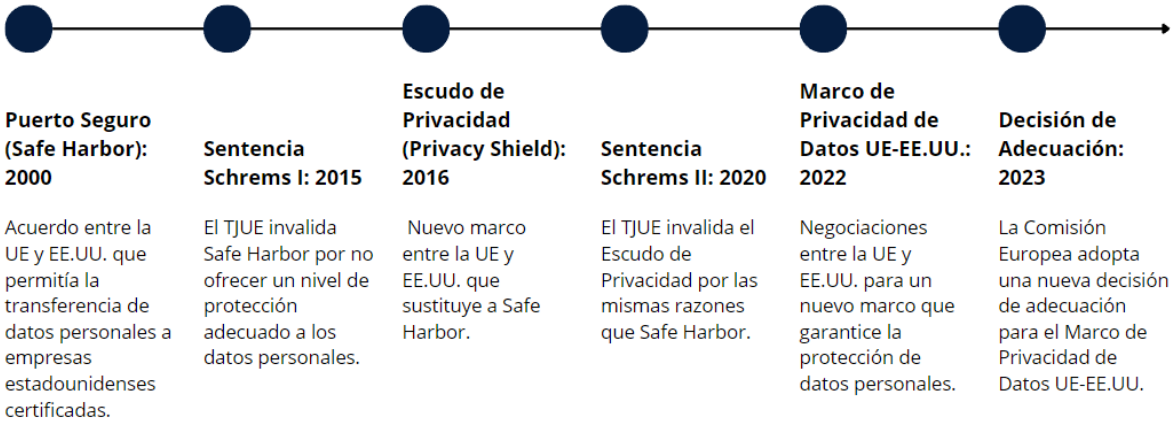
[27] El Reino Unido dejó de formar parte de la UE el 31 de enero de 2020, conforme al Acuerdo sobre la retirada del Reino Unido de Gran Bretaña e Irlanda del Norte de la Unión Europea y de la Comunidad Europea de la Energía Atómica.

(considerandos 14-15). Por tanto, la Comisión considera que el Reino Unido garantiza un nivel de protección equivalente al del RGPD y, además, señala que los mecanismos de supervisión del Reino Unido posibilitan identificar y sancionar las infracciones cometidas (considerando 274).

Decisión de adecuación Unión Europea-Estados Unidos (Data Privacy Framework): un largo camino

La decisión de adecuación Unión Europea-Estados Unidos (en adelante UE-EE.UU) es considerada como la más conflictiva y figurativa a lo largo de los años. La principal disyuntiva entre las partes consiste en que desde EE.UU se considera la normativa europea como muy proteccionista, mientras que los europeos cuestionan si las leyes de EE.UU protegen los datos de los ciudadanos europeos (Sobrino, 2021). En la figura 2, se muestra la línea del tiempo que sintetiza la decisión de adecuación UE-EE.UU.

Figura 5. Línea del tiempo decisión de adecuación UE-EE.UU.



Fuente: elaboración propia.

Por tal motivo, con el fin de conservar la estabilidad y el crecimiento económico de las partes, se confecciona en el 2000 un acuerdo denominado *Safe Harbor* o Puerto Seguro, que permitía transferir de forma legal y con fines comerciales datos personales entre la UE y los EE.UU. Este acuerdo funcionaba a través de un sistema de autocertificación por parte de las empresas de EE.UU, esto implicaba que si las entidades satisfacían ciertos principios podían certificarse para realizar transferencias de datos con la UE. De esta forma, se fomentó en las entidades estadounidenses la autorregulación, ya que la UE consideró la improbabilidad de que se pudiera ejecutar un estatuto general de privacidad en el territorio norteamericano (Sobrino, 2021).

No obstante, la situación de EE.UU cambió en 2013 cuando Edward Snowden, un antiguo empleado de la Agencia Central de Inteligencia reveló "(...) documentos clasificados sobre las actividades de los diferentes servicios de información de EE.UU., en los que se constataba la existencia de programas masivos de vigilancia global" (Sobrino, 2021, p. 232). De esta manera, argumentó que el Puerto Seguro no otorgaba una protección adecuada. Ante esta situación y dada la denuncia interpuesta por Maximillian Schrems, un estudiante austríaco de derecho, el TJUE aseveró que EE.UU participaba en la vigilancia masiva de las personas europeas e invalidó el acuerdo en el 2015 mediante la sentencia Schrems I. Adicionalmente, la sentencia:

> (...) también consideró que se había vulnerado el contenido esencial del derecho a la tutela judicial efectiva… El derecho norteamericano no contemplaba recursos judiciales eficaces para que los ciudadanos europeos pudiesen alegar una vulneración de sus derechos fundamentales en relación con sus datos personales (p. 243).

Esta situación propició un aumento de la inseguridad jurídica en la esfera económica, dadas las disconformidades entre los modelos de protección de datos de la UE y de EE.UU. Lo anterior, impulsó las negociaciones para la elaboración de un nuevo acuerdo en el 2016, denominado *Privacy Shield* o Escudo de Privacidad. El fin de este acuerdo era lograr una equivalencia con el RGPD, una de las similitudes con el *Safe Harbor* es el sistema de autocertificaciones; en el cual, las empresas debían contar con una política de privacidad y renovar de manera anual su afiliación al acuerdo. En cuanto a las reformas:

> Una de las más destacadas fue que los operadores bajo el Escudo de Privacidad se encontraban sujetos a compromisos con respecto a los límites de retención de datos, derechos de acceso, publicidad de políticas de privacidad etc… Además, el Gobierno estadounidense se comprometió a crear un mecanismo de supervisión de las injerencias con fines de seguridad nacional, el Defensor del Pueblo… Otra de las novedades que introdujo el Escudo de Privacidad fue en su ámbito de aplicación, pues afecta tanto a las transferencias internacionales de carácter comercial como al acceso de las autoridades públicas de EE.UU. a los datos transferidos desde la UE, incluso por causas de seguridad nacional (Sobrino, 2021, p. 245).

No obstante y a pesar de las mejoras introducidas en este acuerdo, no se cumplieron los estándares necesarios, lo que ocasionó que el GT29 (2016) detectara una serie de debilidades presentes en el *Privacy Shield*:

> La primera preocupación es que el lenguaje utilizado en el proyecto de decisión de adecuación no obliga a las organizaciones a eliminar los datos si ya no son necesarios. En segundo lugar, el GT29 entiende del Anexo VI que la administración estadounidense no excluye totalmente la recopilación continua de datos masivos e indiscriminados. El tercer punto de preocupación se refiere a la introducción del mecanismo del Defensor del Pueblo. Aunque el GT29 acoge con satisfacción este paso sin precedentes que crea un mecanismo adicional de reparación y supervisión para las personas, sigue preocupado por si el Defensor del Pueblo tiene poderes suficientes para funcionar eficazmente[28] (p. 57).

Por ello, el TJUE ha vuelto a determinar que la decisión de la Comisión Europea sobre el Escudo de Privacidad no se ajusta a la realidad. En otras palabras, EE.UU no protege los datos personales de manera equivalente a la UE. De esta manera, en julio de 2020, el TJUE invalidó el *Privacy Shield* en la Sentencia Schrems II. Tal y como afirma Sobrino (2021):

> Las sentencias Schrems I y II han demostrado que las decisiones de adecuación para la transferencia internacional de datos entre la UE y EE.UU no terminan de cumplir con los estándares europeos del nivel de adecuación, provocando graves riesgos en los derechos de los ciudadanos europeos (p. 252).

Tras la sentencia Schrems II, la UE y EE.UU comenzaron nuevas negociaciones para encontrar un marco legal que permitiera la transferencia de datos personales entre los territorios, ya que para las entidades europeas "(...) esta situación conllevó la necesidad de modificar la forma de relacionarse con las entidades norteamericanas, con un impacto en ocasiones significativo para sus actividades de negocio" (Zorraquino et al., 2023). Es así como en marzo de 2022, la administración Biden y la Comisión Europea anunciaron un acuerdo denominado Marco de Privacidad de Datos UE-EE.UU o *Data Privacy Framework* (DPF), que entró en vigor el 25 de marzo de 2023.

De esta manera, el 10 de julio de 2023 la Comisión Europea adoptó su decisión de adecuación para la circulación de datos UE-EE.UU. relativa al DPF. Esta decisión concluye

[28] Mi traducción. Texto original: "The first concern is that the language used in the draft adequacy decision does not oblige organisations to delete data if they are no longer necessary… Secondly, the WP29 understands from Annex VI that the U.S. administration does not fully exclude the continued collection of massive and indiscriminate data… The third point of concern regards the introduction of the Ombudsperson mechanism. Even though the WP29 welcomes this unprecedented step creating an additional redress and oversight mechanism for individuals, concerns remain as to whether the Ombudsperson has sufficient powers to function effectively".

que EE.UU garantiza un nivel de protección equivalente al de la UE, de acuerdo con la Comisión Europea (2023) el DPF:

> (...) introduce nuevas garantías vinculantes al objeto de dar respuesta a cada uno de los motivos de inquietud puestos de manifiesto por el Tribunal de Justicia de la Unión Europea. Entre estas garantías se encuentran la limitación del acceso por parte de los servicios de inteligencia estadounidenses a los datos de la UE a lo necesario y proporcionado, y el establecimiento de un Tribunal de Recurso en Materia de Protección de Datos, al que los ciudadanos de la UE tendrán acceso (p. 1).

Dentro de las próximas etapas del DPF, la Comisión Europea en conjunto con las autoridades de protección de datos estadounidenses y europeas efectuarán una revisión periódica de su funcionamiento. En este sentido, la primera reunión se realizará antes de que se cumpla un año de la entrada en vigor de la decisión de adecuación, con el fin de comprobar si todos los elementos esenciales funcionan de una manera adecuada. Ante esto, destaca que esta decisión tomada por la UE puede ser retirada si se determina que el nivel de protección resulta ineficiente.

3.3.4. Estándares de Protección de Datos de los Estados Iberoamericanos

Los Estándares de Protección de Datos de los Estados Iberoamericanos, aprobados en 2017, buscan fortalecer la protección de datos personales en la región. La Red Iberoamericana de Protección de Datos, en adelante RIPD establece que:

> (...) los Estándares Iberoamericanos se constituyen en un conjunto de directrices orientadoras que contribuyan a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana de aquellos países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes (p. 3).

Por ello, los Estándares buscan armonizar la normativa en la región y acercarla a los estándares europeos, lo que implica adoptar principios y derechos esenciales de protección de datos personales. El artículo 10.1 de los Estándares establece los principios aplicables al tratamiento de datos personales "(...) el responsable observará los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad" (p. 17). En el capítulo III de los Estándares se determinan los derechos del

titular: de acceso, de rectificación, de cancelación, de oposición, a no ser objeto de decisiones individuales automatizadas, a la portabilidad de los datos personales y a la limitación del tratamiento de los datos personales.

La armonización de la normativa de la región iberoamericana es un proceso complejo que requiere un esfuerzo sostenido y conjunto por parte de todos los actores involucrados. En este sentido, los beneficios potenciales son considerables y pueden contribuir a crear un entorno digital más seguro y confiable para todos los ciudadanos; además, deben verse como una oportunidad para el posicionamiento de la región como un referente en materia de protección de datos. En cuanto a Costa Rica, pese a que el país suscribe los Estándares, la falta de avances en la modernización y actualización de las leyes ha llevado a una situación en la que el derecho a la privacidad de la población no ha alcanzado su pleno desarrollo.

3.3.5. Normativa de países latinoamericanos: caso de Argentina y Uruguay

En este apartado, se examinará la normativa de dos países latinoamericanos, Argentina y Uruguay con respecto a la protección y transferencia internacional de datos personales. Estos países fueron seleccionados debido a que son los únicos en América Latina a los que la UE les ha concedido una decisión de adecuación.

Argentina

En primer lugar, la regulación argentina incorpora de manera implícita la protección de datos personales su la Constitución Nacional de 1853, donde en el artículo 17 se determina la inviolabilidad del domicilio, la correspondencia y los papeles privados, y en el artículo 19 se establece el derecho a la privacidad. Posteriormente, con la reforma de 1994 se incluye la acción de *Habeas Data*, que toda persona puede interponer para:

> (...) tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos.

En el año 2000, Argentina aprueba la Ley de Protección de Datos Personales (LPDP), No. 25.326, la cual tiene por objeto:

> (...) la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos,

o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre (artículo 1).

En cuanto a las transferencias internacionales de datos personales, en el artículo 12.1 de la LPDP se señala que "Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados". Por otra parte, en el año 2001, la LPDP se reglamenta a través del Decreto No.1558/2001[29] y se crea la Dirección Nacional de Protección de Datos, que es la autoridad de aplicación de la LPDP y tiene como fin investigar, controlar y sancionar el tratamiento de los datos personales.

Ahora bien, sobresale que la LPDP y el derecho de *hábeas data* le permite a Argentina en 2003 ser el primero de la región en ser considerado por la UE como un país adecuado para la protección de datos personales, lo que le permitió la libre circulación de datos personales desde la UE hasta Argentina. Más tarde, en 2016, se aprueba la Ley de Acceso a la Información Pública, No. 27.275 con el objetivo de "(...) garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover la participación ciudadana y la transparencia de la gestión pública (artículo 1)".

En el 2017, se crea la Agencia de Acceso a la Información Pública (AAIP), mediante la Ley 27.275 y sustituye a la Dirección Nacional de Protección de Datos. La AAIP "(...) es un ente autárquico con autonomía funcional en el ámbito de la Jefatura de Gabinete de Ministros del Poder Ejecutivo Nacional" (Resolución 94/2023) y cuenta con tres Direcciones Nacionales: la Dirección Nacional de Protección de Datos Personales, la Dirección Nacional de Políticas de Acceso a la Información Pública y la Dirección Nacional de Evaluación de Políticas de Transparencia.

Posteriormente, en el 2018, Argentina se adhiere al Convenio 108 del Consejo de Europa y en noviembre del 2022 se ratifica la adhesión del país al Convenio 108+, lo cual se considera sumamente importante para que el país siga siendo considerado adecuado por la UE en lo concerniente al RGPD. En agosto de 2022, se presenta el anteproyecto de actualización de la Ley 25.326, debido a que la legislación cuenta con más de 20 años de antigüedad. Luego

[29] El Decreto 1158/2001 se encuentra disponible en el siguiente enlace: Decreto 1158/2001. Este decreto fue luego modificado por el Decreto No. 1160/2010 y se encuentra disponible en el siguiente enlace: Decreto 1160/2010.

de la consulta pública donde se recibieron 173 documentos con comentarios y aportes, se presenta un nuevo Proyecto de Ley de Protección de Datos Personales en junio de 2023.

En octubre de 2023 la AAIP a través de la Resolución 198/2023 aprobó las cláusulas contractuales modelo para transferencias internacionales de datos y la Guía de Implementación de la RIPD, siendo el tercer país de la región en acogerse, junto con Uruguay y Perú. Ante esto, la Titular de la AAIP expresó:

> Estas cláusulas son un instrumento para fortalecer la protección de datos personales en los flujos transfronterizos, cuando un Estado no cuenta con la legislación adecuada para las transferencias internacionales. Este es un paso más para promover el desarrollo económico y garantizar la protección de derechos (Gobierno de Argentina, 2023, párr. 2).

Por último, en enero de 2023, la Comisión Europea ratifica que Argentina es un país adecuado para el flujo libre transfronterizo de datos personales. De acuerdo con el Gobierno de Argentina (2024):

> Esta condición impacta de manera positiva y significativa en las relaciones comerciales de Argentina con la Unión Europea (UE), tercer socio comercial que concentra el 10,3% de las ventas argentinas al exterior y el 14,3% de las compras (párr. 1).

En este sentido, la Comisión Europea se encuentra satisfecha con la evolución del marco normativo argentino desde la adopción de la decisión de adecuación en el 2003. Señala dentro de los hitos más importantes del país en este tema: a) la independencia de la AAIP y sus distintas resoluciones, b) la ratificación del Convenio 108 y 108+, y c) el nuevo Proyecto de Ley. La Comisión Europea (2024) visualiza a este último como una oportunidad para reforzar el marco legal argentino de protección de datos.

Uruguay

En Uruguay, el derecho a la protección de datos personales se reconoce como un derecho inherente a la persona en el artículo 72 de la Constitución de la República. Adicionalmente, la Ley de Protección de Datos Personales, No. 18.331 de 2008[30], regula la protección de datos personales y la acción de *habeas data* en concordancia con los principios de: legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos,

[30] Esta Ley se encuentra reglamentada por el Decreto No. 414/009.

reserva y responsabilidad (artículo 5). En el capítulo III de la Ley, se establecen los derechos de los titulares de los datos: de información, de acceso, de rectificación, actualización, inclusión o supresión, a la impugnación de valoraciones personales y a la comunicación de los datos.

En cuanto a la transferencia internacional de datos personales, el artículo 23 señala que "Se prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia". Por otra parte, a través de la Ley 18.331 se crea la Unidad Reguladora y de Control de Datos Personales (URCDP), con autonomía técnica y facultades de investigación, intervención y sanción para garantizar el cumpliento de la normativa.

Por ello, en 2012, Uruguay fue reconocido por la UE[31] como un país con un nivel de protección adecuado de los datos personales. De esta manera, en 2013 logra la adhesión al Convenio 108 y se convierte en el primer país no europeo en formar parte del Convenio y de su Protocolo Adicional (aprobado por la Ley 19.030). Posteriormente, la Ley 18.331 sufre dos modificaciones, una en 2018 y otra en 2020; de esta manera, se amplía el ámbito de aplicación fuera del territorio uruguayo, se crean nuevas obligaciones para responsables y encargados de bases de datos y se constituye la figura del delegado de protección de datos.

En 2021, Uruguay vuelve a ser el primer país de América Latina en ratificar el Convenio 108+ mediante la Ley 19.948. Por último, en 2024, Uruguay es ratificado por la Comisión Europea como un país con un nivel adecuado para la protección de datos. Para esto, la Comisión Europea consideró el desarrollo del marco normativo de Uruguay desde la adopción de la decisión de adecuación en 2012: a) las modificaciones a la Ley 18.331, b) la adhesión al Convenio 108 y 108+, y c) la consideración de que las autoridades públicas del país se encuentran sujetas a normas claras, precisas y accesibles.

3.3.6. Forjando un modelo latinoamericano de adecuación

Desarrollar un marco regional latinoamericano de adecuación para la transferencia internacional de datos personales podría convertirse en una realidad, que permitiría el libre flujo de datos personales entre los países de la región, al tomar como referencia los procesos de adecuación que se encuentran vigentes alrededor del mundo. En este sentido, contar con un estándar latinoamericano podría fortalecer a la región, ya que debido al valor económico que

[31] Decisión No.2012/484/UE.

han alcanzado los datos personales, su regulación es un elemento esencial para lograr la soberanía digital al mismo tiempo en que se promueve el comercio y la inversión extranjera directa. De acuerdo con Belli et al. (2023):

> El continente americano, por su ubicación geográfica, se convierte en un punto de encuentro entre los cinco continentes, por lo que establecer un estándar común facilitaría el tratamiento y flujo de datos personales, en un ejercicio que beneficiará a todos los involucrados, desarrolladores, sector privado y el usuario final de los productos y servicios que se ofrecen (p. 5).

Es así como, los autores destacan que un modelo latinoamericano de adecuación podría gestarse a través una serie de acciones que se listan a continuación:

a. Efectuar un tratado regional de protección de datos personales a nivel latinoamericano.

b. Reconocer la existencia y la aplicación de tratados internacionales vigentes sobre derechos humanos y sobre la protección de datos personales como el Convenio 108 y 108+.

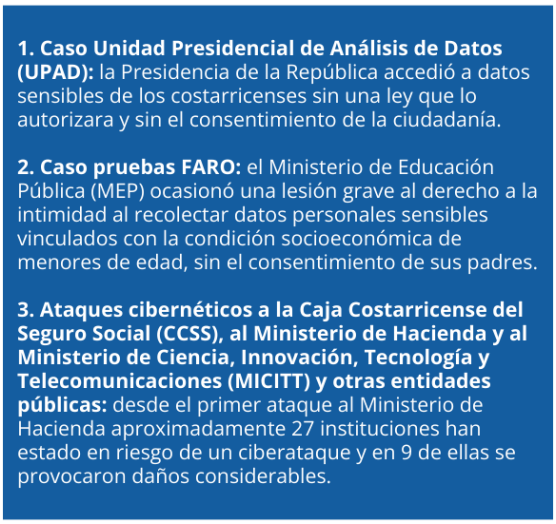
c. Generar un marco general para el reconocimiento de adecuación a partir de un *checklist* que podría ser confeccionado por la RIPD o también a través de un acuerdo entre las agencias de datos personales de la región.

d. Crear y promover el uso de cláusulas contractuales modelo y normas corporativas vinculantes para la región. La RIPD creó una primera versión de las cláusulas contractuales modelo, así como una guía para su implementación; sin embargo, únicamente Perú y Uruguay se han acogido al modelo.

3.4. Marco normativo costarricense existente en materia de transferencia internacional de datos personales

En esta sección, se describe el marco normativo costarricense en materia de transferencia internacional de datos personales, con el fin de determinar si en Costa Rica existe un marco institucional que facilite las transferencias internacionales con terceros países, y que al mismo tiempo vele por la protección de la privacidad y la intimidad de las personas. En el país, se han gestado en los últimos años casos que revelan un manejo inadecuado de los datos personales de las personas (figura 3), por lo tanto, la temática en torno a su protección ha tomado especial relevancia.

Figura 6. Ejemplos de casos de manejo inadecuado de datos personales en Costa Rica



Fuente: elaboración propia con base en Ramírez (2023).

3.4.1. Ley de Protección de la Persona frente al tratamiento de sus datos personales No. 8968 y su Reglamento

Esta Ley se encuentra vigente desde el año 2011 y emana de la necesidad que tenía el Estado de garantizar la protección de los ciudadanos con respecto al tratamiento de sus datos personales a través de un marco regulatorio, dado el auge de la era de los datos y de las innovaciones tecnológicas. El objetivo de la Ley No. 8968 es garantizar a cualquier persona:

> (...) su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes (artículo 1).

Ahora bien, en cuanto al ámbito de la transferencia internacional de datos, la Ley en cuestión no distingue si este aspecto queda regulado únicamente a nivel nacional o si también atañe a las transferencias internacionales. Al respecto, la Ley indica que:

> Los responsables de las bases de datos, públicas o privadas, sólo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley (artículo 14).

Aunado a lo anterior en el Reglamento a la Ley No. 8968 se establece en el artículo 40 que la transferencia de datos personales necesitará siempre del consentimiento informado del titular, salvo que exista una disposición legal que indique lo contrario. Por otro lado, en el artículo 15 de la Ley se crea la Agencia de Protección de Datos de los Habitantes (Prodhab)[32] como un órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz, con independencia de criterio y personalidad jurídica instrumental propia en el desempeño de sus funciones y en la administración de sus recursos y presupuesto. Es así, como su fin es el de garantizar a todas las personas su derecho a la autodeterminación informativa, la defensa de su libertad y la igualdad con respecto al tratamiento de sus datos.

Por lo tanto, cabe destacar que la posición normativa que involucra la transferencia de datos internacionales no es clara y merece atención. La escasez de una distinción explícita entre las transferencias nacionales e internacionales deja un vacío hacia diversas interpretaciones y suscita interrogantes sobre la aplicación efectiva de las disposiciones legales en la esfera global.

3.4.2. Protección de datos personales: una comparativa entre Costa Rica, Argentina y Uruguay

A continuación, se muestra en la tabla 5 una comparación entre Costa Rica, Argentina y Uruguay sobre la protección de datos personales (legislación, autoridades de control y compromisos internacionales):

a. Legislación: los tres países cuentan con una ley que protege los datos personales, siendo Argentina el primero en aprobarla, en el año 2000.

b. Autoridades de control: los tres países tienen una autoridad de control; sin embargo, en Costa Rica, la Prodhab se encuentra adscrita al Ministerio de Justicia y Paz, por lo que no cuenta con autonomía en sus funciones.

[32] Órgano rector en materia de privacidad en Costa Rica.

c. Compromisos internacionales: Costa Rica no se encuentra adherido al Convenio 108 y 108+, mientras que Argentina y Uruguay si, siendo este último el primero en adherirse en el 2013.

Tabla 5. Comparativa entre Costa Rica, Argentina y Uruguay sobre la protección de datos

Elemento a comparar	Costa Rica	Argentina	Uruguay
Legislación	Ley de Protección de la Persona frente al tratamiento de sus datos personales No. 8968 de 2011	Ley de Protección de Datos Personales (LPDP), No. 25.326 del 2000	Ley de Protección de Datos Personales, No. 18.331 de 2008
Autoridades de control	Agencia de Protección de Datos de los Habitantes adscrito al Ministerio de Justicia y Paz	Agencia de Acceso a la Información Pública con autonomía	Unidad Reguladora y de Control de Datos Personales con autonomía técnica y capacidad de sanción
Compromisos internacionales	No está adherido al Convenio 108 y 108+	Convenio 108 y 108+	Convenio 108 y 108+

Fuente: elaboración propia

Los tres elementos que se comparan son algunos de los factores que la UE considera al tomar una decisión sobre la adecuación. En este contexto, se evidencia una disparidad entre Costa Rica y los países analizados, principalmente en lo que respecta a la autoridad de control y los compromisos internacionales.

3.4.3. Proyecto de Ley No. 23097: Ley de Protección de Datos Personales

El Proyecto de Ley bajo el expediente No. 23097 fue presentado por el diputado del Partido Liberal Progresista (PLP), Eliecer Feinzaig y otros diputados; este surge con el objetivo de realizar una reforma al marco regulatorio existente por cuatro razones principales, siendo dos de estas concernientes a la transferencia internacional de datos:

a. La legislación costarricense existente se inspiró en la española, específicamente en Ley Orgánica de Protección de Datos No.15/1999 y esta Ley fue derogada y sustituida por el Reglamento General de Protección de Datos Personales (RGPD). Por tal razón, gran cantidad de países a nivel mundial y regional han adecuado sus legislaciones internas a lo enmarcado por el RGPD y Costa Rica no debería ser una excepción.

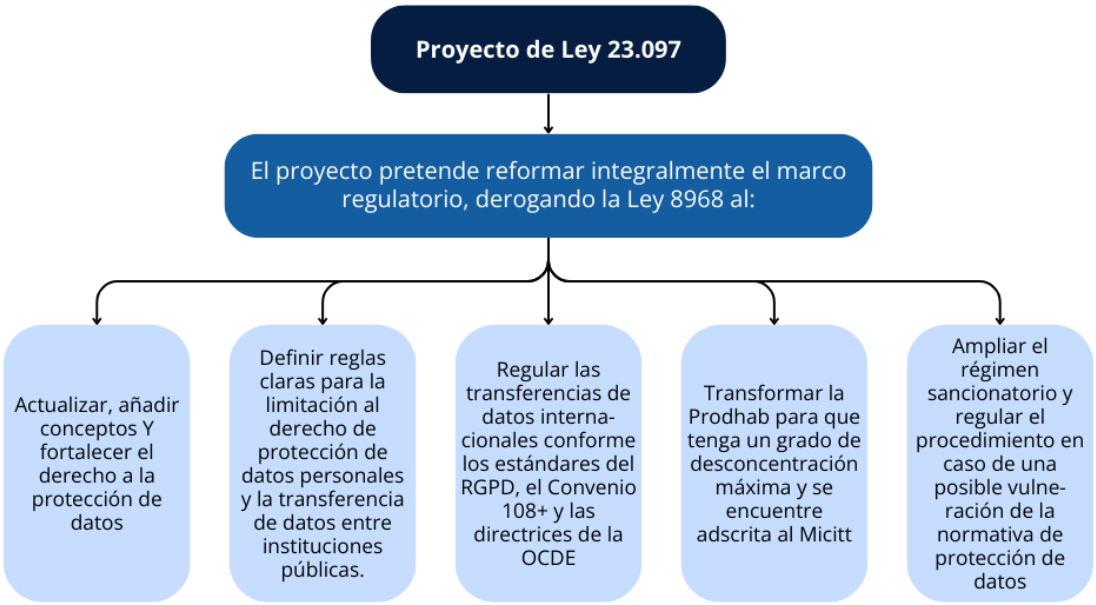
b. Costa Rica manifestó la intención de adherirse al Convenio 108 y al Protocolo 108+, siendo el primer y único tratado internacional jurídicamente vinculante que aborda de manera específica la protección de datos personales. Formar parte del Convenio le posibilitaría a Costa Rica gestionar una decisión de adecuación del Consejo de Europa, lo que le permitiría considerarse como un puerto seguro para las transferencias internacionales de datos personales.

c. La Organización para la Cooperación y el Desarrollo Económicos (OCDE) tiene directrices específicas[33] con respecto a la protección de datos, dirigidas especialmente hacia la transferencia internacional de datos personales.

d. Después de una década de existencia, la legislación costarricense ha incidido de forma modesta en la manera en que se tratan los datos personales, por lo que, no se ha propiciado un desarrollo efectivo del derecho a la privacidad de las personas.

El texto del Proyecto se compone de 83 artículos y 6 transitorios contenidos en 11 capítulos. Dentro de los principales aspectos que contempla el Proyecto, destacan:

Figura 7. Resumen del Proyecto de Ley 23.097



Fuente: elaboración propia con información del informe jurídico del texto sustitutivo de la Asamblea Legislativa, expediente No. 23.097.

[33] i) Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, de 1980, ii) Declaración sobre flujos de datos transfronterizos, de 1985, y iii) la Declaración ministerial sobre la protección de la privacidad de las redes globales, de 1998.

El Proyecto de Ley incorpora en el capítulo V las transferencias internacionales de datos personales. En el artículo 45 se establecen las reglas generales para efectuar una transferencia internacional de datos personales:

a. Cuando el responsable cuente con el consentimiento informado del titular de los datos.

b. Cuando la transferencia sea exigida legalmente o en un tratado internacional del que la República de Costa Rica sea parte, para la investigación y persecución de los delitos, así como la administración de justicia o por razones de seguridad nacional.

c. Cuando el país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte de la Agencia de Protección de Datos, o bien, el país destinatario acredite condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado.

d. Cuando el exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y acredite el cumplimiento de las condiciones mínimas y suficientes aplicables a la materia.

e. Que se encuentre prevista en una ley o tratado internacional del que la República de Costa Rica sea parte.

Adicionalmente, este Proyecto de Ley plantea una reestructuración de la Prodhab y destaca los desafíos de esta entidad desde su creación, entre los que destacan: una alta rotación de sus directores; recursos humanos, económicos y tecnológicos limitados; la dependencia de la Prodhab al Ministerio de Justicia y Paz, el cual no tiene vinculación directa con temas tecnológicos y que, además, le ha restado independencia de criterio. Estos cambios se incluyen en el capítulo VIII del Proyecto.

El artículo 61 se centra en las disposiciones generales; en primer lugar, se establece que la Agencia será un órgano adscrito al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt); que contará con desconcentración máxima, idoneidad especial y técnica e independencia operativa, técnica, administrativa, presupuestaria y funcional. Adicionalmente, podrá dictar reglamentaciones específicas a la Ley en cuestión concernientes a la materia de su especialidad. Por otra parte, se determina que la Agencia tendrá personalidad jurídica instrumental, lo que le permite celebrar contratos y convenios con entidades públicas

o privadas a nivel nacional e internacional; también, su facultad le permite sancionar cualquier conducta que se catalogue como una violación de los derechos de las personas a la protección de sus datos personales.

3.4.4. Recomendaciones de la OCDE para Costa Rica

Costa Rica se convirtió en un miembro oficial de la OCDE el 25 de mayo de 2021, tras un proceso de cinco años en los cuales el país se sometió a revisiones técnicas profundas. En cuanto al tema de la privacidad, la Organización determina que el país cubre los principios básicos de las Directrices de Privacidad de la OCDE; sin embargo, se señala que el régimen de privacidad de Costa Rica es incipiente. Por lo tanto, las recomendaciones de la OCDE para el país son las siguientes:

a. Finalizar la estrategia de privacidad PRODHAB que refleje un enfoque coordinado entre organismos gubernamentales.

b. Desarrollar e implementar metodologías para supervisar y evaluar las actividades de protección de datos a fin de fundamentar las políticas.

c. Adoptar las medidas adecuadas para facilitar la cooperación transfronteriza en materia de aplicación de la legislación sobre privacidad.

3.5. Reflexiones del capítulo

a. El intercambio comercial entre la UE y Costa Rica ha experimentado un notable crecimiento desde la firma del AACUE, lo que convierte a la región europea en un importante socio comercial para Costa Rica.

b. La transmisión de datos personales a nivel internacional entre países y empresas se ve impulsada por la necesidad de adecuarse a un contexto globalizado y crear oportunidades de negocio y crecimiento a escala global.

c. El marco institucional internacional proporciona una comprensión fundamental sobre los diversos acuerdos, estándares, directrices y marcos legales a nivel global para abordar la transferencia internacional de datos personales. En este contexto, el RGPD garantiza el derecho a la protección de datos y destaca en uno de sus considerandos la relevancia de los flujos de datos transfronterizos para la promoción del comercio. Sin

embargo, solo permite el intercambio de datos si el país tercero asegura un nivel de protección adecuado.

d. En América Latina, sólo Uruguay y Argentina han sido reconocidos por la Unión Europea como países que ofrecen garantías adecuadas para la transferencia internacional de datos personales. Esto se debe a su legislación, la existencia de agencias de protección de datos autónomas, y la ratificación de compromisos internacionales como el Convenio 108 y 108+. En contraste, Costa Rica enfrenta desafíos, especialmente en lo que respecta a la autoridad de control y la adhesión a compromisos internacionales, como se analizará posteriormente.

Capítulo IV: El flujo transfronterizo de datos personales desde la UE hacia un tercer país, las decisiones de adecuación y los mecanismos alternativos

En el presente capítulo se estudiarán las decisiones de adecuación y los mecanismos alternativos para la transferencia internacional de datos personales entre la UE y un tercer país. Por ello, el capítulo se estructura de la siguiente manera: a) el punto de partida de la protección de datos en la UE, b) la influencia del RGPD en las prácticas de transferencia internacional de datos a nivel global, c) las fortalezas y debilidades de la legislación europea con respecto al intercambio transfronterizo de datos, d) las decisiones de adecuación (criterios para su determinación, proceso e implicaciones para los países que no logran una decisión de adecuación) y e) los mecanismos alternativos para la transferencia internacional de datos personales. Para alcanzar este objetivo, se efectúo una revisión documental y también se toma en cuenta la información recopilada a través de las entrevistas.

4.1. El punto de partida de la protección de datos en la UE

La protección de los datos personales "(...) forma parte de los fundamentos constitucionales comunes de Europa y lleva más de veinte años ocupando un lugar destacado en el Derecho de la Unión" (Comisión Europea, 2017, p. 2). Lo anterior, se refleja desde la introducción de la Directiva 95/46 hasta la adopción del RGPD de 2016 y su posterior actualización, el RGPD de 2018. No obstante, la preocupación por la protección de datos personales no es un fenómeno que se limita únicamente al territorio europeo, por el contrario, es un desafío global.

A pesar de esto, existen enfoques normativos divergentes que dan lugar a niveles dispares de protección entre jurisdicciones, lo que genera de acuerdo con la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, UNCTAD (2016) "(...) la necesidad de controles legales sobre los flujos transfronterizos de datos personales entre jurisdicciones, con el fin de evitar que se eludan las leyes del régimen más protector y se erosionen los derechos de privacidad de las personas"[34] (p. 3). En este sentido, la UE proporciona una serie de

[34] Mi traducción. Texto original: "This, in turn, leads to the need for legal controls over cross-border flows of personal data between jurisdictions, in order to prevent the laws of the more protective regime from being circumvented and the privacy rights of the individuals being eroded".

mecanismos que permiten las transferencias internacionales de datos que se abordarán en este capítulo.

4.2. La influencia del RGPD en las prácticas de transferencia internacional de datos a nivel global

La implementación del RGPD ha marcado un punto de inflexión en las prácticas de transferencia internacional de datos personales a nivel mundial, sea esta influencia positiva o negativa, dependiendo desde la óptica de la cual se visualice. Esta normativa europea fue diseñada para fortalecer la protección de los datos de los ciudadanos de la UE; sin embargo, ha tenido un impacto considerable en cómo los países y las empresas gestionan y transfieren datos más allá de sus fronteras.

A partir de las entrevistas realizadas se obtienen distintas perspectivas sobre la influencia que el RGPD ha tenido en los flujos transfronterizos de datos personales (figura 8). Se destaca la importancia del RGPD como un punto de referencia en el ámbito de la protección de datos y se le compara con un "oráculo normativo", sugiriendo que es una autoridad suprema en la materia. Adicionalmente, se le describe como un "parteaguas", lo que significa que marca un cambio significativo en la protección de datos y como un "faro" que proporciona orientación. Asimismo, se reconoce el impacto que ha tenido el Reglamento en las prácticas globales de transferencia de datos, haciendo hincapié en que ha generado cambios en las empresas, mejorando las prácticas empresariales relacionadas con la protección de los datos.

Por otro lado, se señala que muchas jurisdicciones alrededor del mundo se están adaptando para cumplir con los estándares del RGPD si desean hacer negocios con Europa. Esto implica que el RGPD no solo influye en la Unión Europea, sino que también ejerce un efecto notable en la regulación global de protección de datos. Varios países están buscando ajustar sus normativas para cumplir con los estándares del RGPD, con el objetivo de facilitar el comercio y las relaciones comerciales con Europa. No obstante, se encuentra una visión crítica hacia el RGPD, ya que si bien, se ve a la UE como una referencia en la materia de protección de datos personales; también puede ser percibida como una barrera para el comercio y la inversión debido a las regulaciones asociadas, lo que puede crear obstáculos o dificultades adicionales para las empresas que buscan operar en el mercado europeo.

Un ejemplo de la influencia del RGPD, puede visualizarse con EE.UU, quién ha abogado históricamente por un modelo de transferencias abiertas de datos como se abordó

anteriormente; sin embargo, a raíz de la necesidad de efectuar negocios con la UE que involucran la transferencia internacional de datos personales, ha tenido que ceder y comenzar a tener un modelo de protección de datos más europeo. Lo anterior, se ejemplifica con la implementación inicial del acuerdo Puerto Seguro en el 2000, posteriormente con el Escudo de Privacidad en 2016 y ahora con el Marco de Privacidad de Datos UE-EE.UU.

Figura 8. Influencia del RGPD en la transferencia internacional de datos a nivel global

"El Reglamento General de Protección de Datos de la Unión Europea es casi como el oráculo normativo en materia de protección de datos. El influjo de la regulación europea a nivel global en materia de protección de datos es por excelencia el más notable y el más reconocido".

Garro (comunicación personal, 7 de febrero de 2024)

"Para mí, el Reglamento General de Protección de Datos de la Unión Europea llega a ser un parteaguas en este tema, llega a proveer no solamente a la Unión Europea, sino que a los demás países una luz, un faro; llega a establecerse como el documento referencia por los demás países".

Durán (comunicación personal, 7 de febrero de 2024)

"Sin duda la influencia del Reglamento en las prácticas globales de transferencia de datos ha sido de un impacto muy grande porque generó cambios en las prácticas de las empresas al establecer estándares muy altos, muy estrictos para la protección de datos personales".

Ross (comunicación personal, 1 de marzo de 2024)

"Yo he de decir que hasta hoy, yo he visto que la Unión Europea es una referencia, pero, no creo que sea del todo positiva. Creo que se ve como una barrera y una barrera al comercio y a la inversión".

Persona entrevistada (comunicación personal, 28 de febrero de 2024)

"El Reglamento, para mi, ha ocasionado que a nivel mundial además de marcar el norte de los países de hacia dónde deberíamos ir, ha elevado los estándares de protección de datos, lo que ha originado que muchas jurisdicciones se adapten si quieren hacer negocios con Europa".

Lemaitre (comunicación personal, 6 de marzo de 2024)

Fuente: elaboración propia con información tomada de las entrevistas realizadas.

Sin duda, el RGPD ha generado un impacto en la gestión y protección de datos a nivel mundial. Si bien ha promovido avances significativos en la protección de datos y ha establecido un estándar en este ámbito, también ha planteado desafíos y preocupaciones en cuanto a su implementación y sus implicaciones comerciales. Su influencia continuará siendo tema de discusión a medida que avance el panorama de la protección de datos y la regulación internacional.

4.3. Fortalezas y debilidades de la legislación europea con respecto al intercambio transfronterizo de datos personales

Como se mencionó anteriormente, la legislación europea en materia de intercambio transfronterizo de datos ha sido objeto de atención, especialmente en un contexto marcado por la era de los datos. En este sentido, resulta importante conocer las fortalezas y las debilidades de esta legislación (tabla 6). En términos de fortalezas, sobresale el enfoque integral con respecto a la protección de datos, ya que ofrece un marco legal completo. Además, posiciona al ciudadano en el centro de la protección de datos al ampliar los derechos que las personas tienen sobre sus datos (acceso, control, rectificación, oposición, supresión, portabilidad, etc.). Por otra parte, facilita la estandarización y simplifica el intercambio de datos entre los países miembros y los que se adecuan a su normativa. Al respecto, Durán (comunicación personal, 7 de febrero de 2024) indica que:

> Se empiezan a hablar con el mismo nombre y a llamar con los mismos apellidos algunos procesos que anteriormente en algún país se hacía de una forma y en otros de otra. Entonces, eso fortalece no solamente la transferencia en el sentido amplio de la palabra, sino, también en su sentido más estricto, la facilita. Ya entendemos de qué estamos hablando cuando estamos haciendo "x" o "y". Entonces, creo que para el comercio internacional ha sido una de las mayores ventajas.

Ahora bien, sobresalen como debilidades de la legislación europea en cuanto al intercambio transfronterizo de datos los costos de cumplimiento y las sanciones, especialmente para las pequeñas y medianas empresas (PYMEs). Puede ser muy costoso asegurar la conformidad con el RGPD, porque implica la contratación de personal especializado y la inversión en sistemas y en mecanismos alternativos para la transferencia de datos personales si el país en el que se encuentran no cuenta con una decisión de adecuación. Aunado a lo anterior, es posible que exista una complejidad en la adaptación a la norma, debido a que puede resultar difícil de comprender y de aplicar adecuadamente. Por otra parte, esta legislación también puede visualizarse como una barrera comercial al obstaculizar el intercambio de datos y con ello el comercio internacional.

Tabla 6. Fortalezas y debilidades de la legislación europea relacionadas con la transferencia internacional de datos personales

Fortalezas	Debilidades
1. Enfoque integral respecto a la protección de datos. 2. Centrado en el ciudadano. 3. Permite una estandarización.	1. Los costos de cumplimiento y las sanciones pueden ser muy altas 2. Existe una complejidad en la adaptación a la norma. 3. Se puede visualizar como una barrera al comercio.

Fuente: elaboración propia con información tomada de las entrevistas realizadas.

4.4. Las decisiones de adecuación

Las decisiones de adecuación permiten que se efectúe una libre circulación de datos personales desde la UE hacia un tercer país, región u organización internacional fuera del EEE, sin la necesidad de aportar ninguna garantía extra ni cumplir con otros requisitos. Obtener una decisión de adecuación implica que se cuenta con un nivel de protección sustancialmente equivalente al de la UE, de acuerdo con Gónzalo (2019):

> La consideración de "adecuado" se logra mediante una combinación de derechos para los afectados y obligaciones para los responsables del tratamiento y qué tipo de organismo puede hacer cumplir los derechos, y sobre todo el sistema que garantice la efectividad de la legislación vigente (p. 356).

Para ello la Comisión Europea evalúa: a) el marco jurídico en general, b) la existencia y funcionamiento de una o varias autoridades de control independientes y c) los compromisos internacionales asumidos u obligaciones derivadas de acuerdos o de instrumentos jurídicamente vinculantes (GT29, 2018). Se profundizará en estos requisitos más adelante.

Una característica de las decisiones de adecuación es su flexibilidad, ya que pueden hacer referencia tanto a una adecuación total del territorio como a una adecuación parcial. Por ejemplo, la decisión sobre Canadá comprende únicamente a las entidades privadas que se encuentran en el ámbito de aplicación de la Ley canadiense relativa a la protección de la información personal y a los documentos electrónicos, *Personal Information Protection and Electronic Documents Act* (Comisión Europea, 2017). La Comisión Europea (2017) se refirió a este tema indicando que:

> En algunos casos, en lugar de adoptar un enfoque nacional, puede resultar más adecuado recurrir a otras opciones, como la adecuación parcial o sectorial (por ejemplo,

en el ámbito de los servicios financieros o de las tecnologías de la información), que puedan abarcar zonas geográficas o sectores industriales que representan una parte importante de la economía de un determinado tercer país (p. 9).

4.1.1. Criterios para determinar una decisión de adecuación

El Reglamento no establece cómo se debe de iniciar un proceso de adecuación, por ello, tal como señala Gonzalo (2019) "Los elementos, principios y condiciones que se tienen en cuenta para determinar a un tercer Estado, región u organización internacional como seguro se encuentran en varios documentos tanto normativos como recomendaciones de diferentes organismos de la Unión Europea" (p. 356). La práctica habitual consistía en que el país externaba su interés de obtener la adecuación a la Comisión Europea, y de esta manera se comenzaba el proceso.

De acuerdo con el comunicado sobre Intercambio y Protección de Datos Personales en un Mundo Globalizado, la práctica parece estar cambiando, ya que la Comisión considera que deben examinarse una serie criterios al momento de determinar los terceros países con los que le conviene entablar un diálogo sobre adecuación:

a. El alcance de las relaciones comerciales (efectivas o posibles) de la UE con un determinado tercer país, incluida la existencia de un acuerdo de libre comercio o de negociaciones en curso.

b. La magnitud de los flujos de datos personales con origen en la UE, que reflejan lazos geográficos o culturales.

c. Si el tercer país es pionero en el ámbito de la protección de datos y la privacidad y puede servir de modelo para otros países de su región.

d. La relación política global con el tercer país en cuestión, en particular por lo que respecta al fomento de valores comunes y objetivos compartidos a escala internacional (Comisión Europea, 2017, p. 9).

No obstante, la Comisión indica que atenderá las manifestaciones de interés de otros países que busquen una decisión de adecuación; además menciona que la adecuación implica un diálogo específico y cooperación con el país interesado (Comisión Europea, 2017). Ahora bien, se profundizará en los criterios que la Comisión Europea toma en cuenta al evaluar una

posible decisión de adecuación que se encuentran en el artículo 45, inciso 2 del RGPD 2016/679:

a. El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos

b. La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros

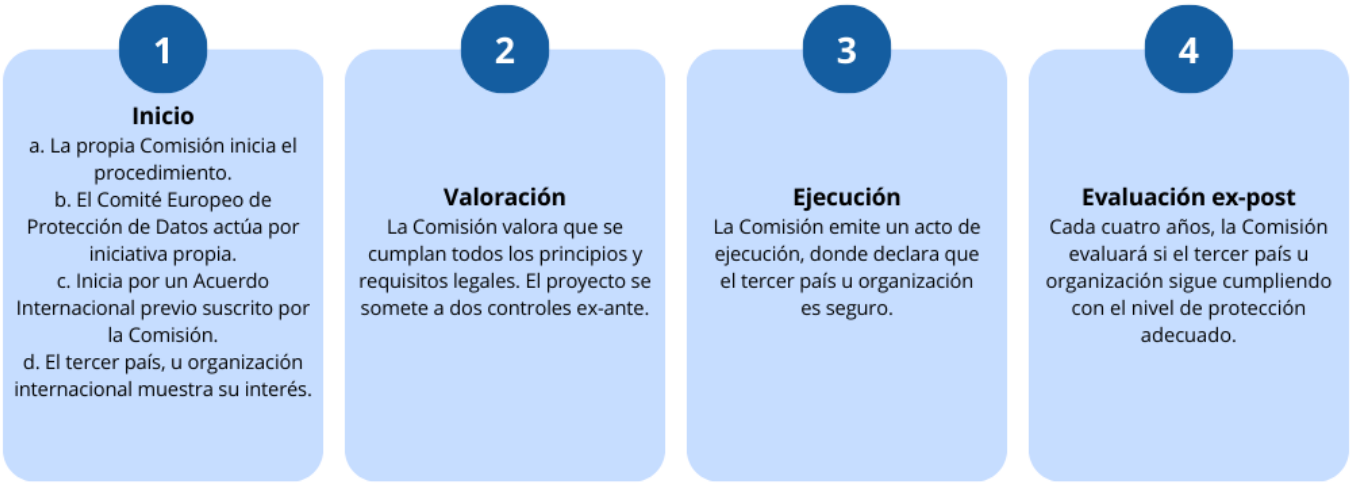
c. Los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

En este sentido, de acuerdo con el GT29 (2018) “queda claro que cualquier análisis significativo de la protección adecuada debe incluir dos elementos básicos: el contenido de las normas aplicables y los medios para garantizar su aplicación efectiva” (p. 3).

4.1.2. Proceso para lograr una decisión de adecuación

Como se mencionó anteriormente, si bien el RGPD no explica el proceso para iniciar y lograr una decisión de adecuación, en la figura 7, se sintetizan las 4 etapas principales del proceso para lograr una decisión de adecuación, estas se extraen de la investigación de Gonzalo (2019):

Figura 9. Proceso para lograr una decisión de adecuación



Fuente: elaboración propia

En primer lugar, el proceso lo puede comenzar la Comisión Europea de acuerdo con los criterios señalados anteriormente sobre la conveniencia de entablar un diálogo sobre adecuación; por otra parte, el Comité Europeo de Protección de Datos puede actuar por iniciativa propia (artículo 70.1, inciso s del RGPD de 2016). También puede iniciar por un Acuerdo Internacional previo suscrito por la Comisión, esto sucedió con el Acuerdo entre EE.UU y la UE, que dio lugar a la aprobación del Escudo de Privacidad, lo mismo sucedió con el Tratado de Libre Comercio firmado con Japón. Por último, el proceso puede dar inicio por el interés del tercer país u organización internacional.

Posteriormente, se realiza una valoración del cumplimiento de principios y requisitos legales por parte de la Comisión. Adicionalmente, el proyecto se somete a dos controles ex-ante:

a. Procedimiento de examen: es de carácter general, el proyecto debe someterse al dictamen de un comité de representantes de los miembros de la Unión Europea, si una mayoría cualificada[35] vota a favor, se adopta; si la mayoría vota en contra, la Comisión no puede adoptarlo. Por otra parte, si no hay una mayoría ni a favor ni en contra, la Comisión puede adoptarlo o puede presentar una nueva versión. En este procedimiento se analiza la compatibilidad con el derecho de la UE.

[35] El 55% de los países de la UE que representen como mínimo al 65% de la población total de la UE.

b. Control técnico: el Comité Europeo de Protección de datos emite un dictamen sobre la adecuación del tercer país u organización internacional. En este control se presta atención a la compatibilidad con la protección del dato.

Una vez que se haya tomado la decisión, la Comisión emite un acto de ejecución, la decisión de adecuación, en la que declara que el tercer país u organización internacional es segura y tiene un nivel adecuado de protección de datos. En esta decisión, se estipula el ámbito de aplicación territorial y sectorial, así como las autoridades independientes. Por último, al menos cada cuatro años, la Comisión debe efectuar una evaluación ex-post, con el fin de determinar si se sigue cumpliendo con el nivel adecuado de protección de datos; si no lo cumple, la Comisión puede derogar, suspender o modificar la decisión.

Cabe destacar que las decisiones de adecuación no pueden ser objeto de negociación en un acuerdo de libre comercio, debido a que son una decisión unilateral adoptada por la Comisión. De acuerdo con la Comisión Europea (2017):

> (...) las decisiones de adecuación, inclusive las de carácter parcial o sectorial, son la mejor manera de fomentar la confianza mutua y garantizar la libre circulación de datos personales, favoreciendo así los intercambios comerciales que conllevan transferencias de datos personales al tercer país interesado. Por tanto, estas decisiones pueden facilitar las negociaciones comerciales o complementar los acuerdos comerciales vigentes, de modo que puedan resultar más beneficiosos (p. 10).

4.1.3. Implicaciones para los países que no logran una decisión de adecuación

El no lograr una decisión de adecuación con la UE puede conllevar una serie de repercusiones sobre todo en términos de comercio (figura 10). Al respecto, Lemaitre (comunicación personal, 6 de marzo de 2024) señala que:

> Esto tiene implicaciones para las empresas y para los países. Estamos hablando de perder el mercado europeo en temas de gestión de servicios, por ejemplo, lo que puede tener impactos comerciales negativos y además requerir inversiones adicionales en mecanismos de transferencias de datos.

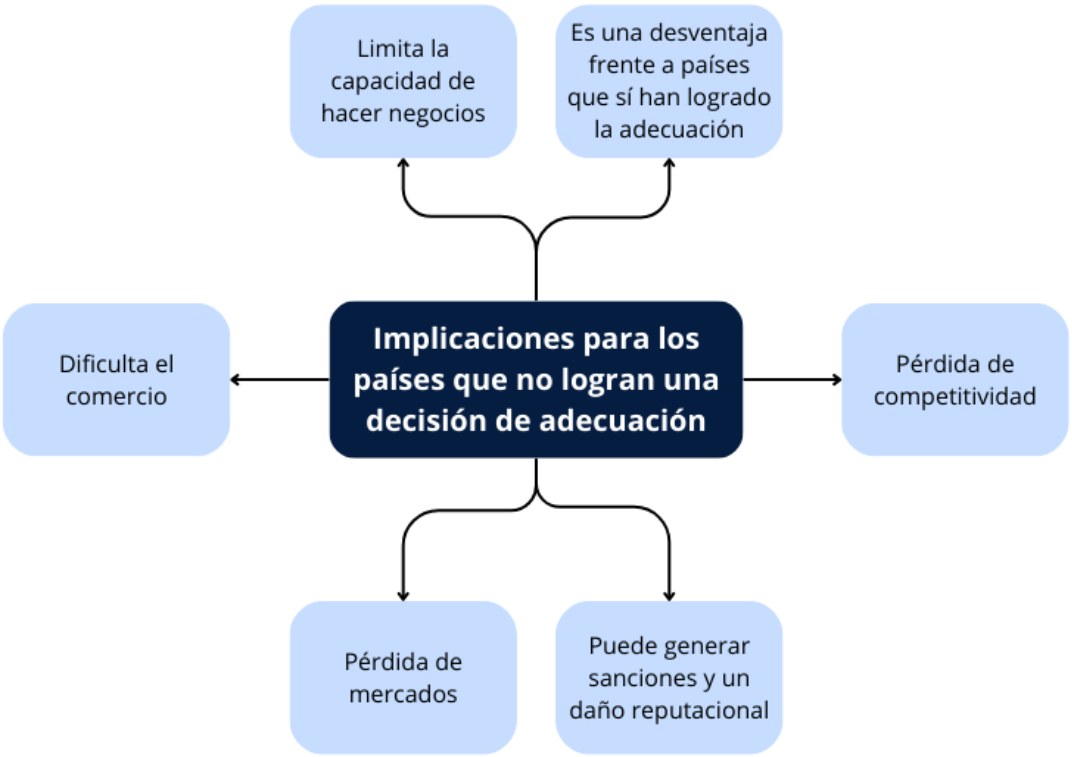
Aunado a lo anterior, limita la capacidad de los países de hacer negocios y de expandir su inversión extranjera directa. A su vez, se pierde competitividad y pone al país en desventaja con otros que sí han logrado la adecuación. Por ejemplo, el funcionario de COMEX

(comunicación personal, 28 de febrero de 2024) menciona que muchas empresas de servicios decidieron instalarse en Uruguay en lugar de Costa Rica, la diferencia entre ambos países radicó en que uno sí contaba la decisión de adecuación y el otro no. Adicionalmente, Durán (comunicación personal, 7 de febrero de 2024) indica que el no contar con una decisión de adecuación:

> Genera una pérdida del comercio no solo con la Unión Europea, sino con países que no están en la Unión Europea, pero que sí tienen su normativa adecuada y estandarizada. Entonces no solamente perdés en la vía del comercio ida y vuelta hacia Europa, sino que también con los países que ya han estado elevando sus estándares sobre esto.

Adicionalmente, el incumplimiento de la normativa europea puede conllevar sanciones severas cuando se transfieren datos personales sin un mecanismo alternativo. Estas sanciones, que suelen ser considerables, no solo impactan financieramente a las empresas, sino que también pueden dañar su reputación debido a la pérdida de confianza de los consumidores. En este contexto, la conformidad con las normativas europeas de protección de datos se vuelve crucial no solo desde un punto de vista legal, sino también como un medio para resguardar la reputación y la viabilidad empresarial.

Figura 10. Implicaciones para los países que no logran una decisión de adecuación



Fuente: elaboración propia con información tomada de las entrevistas realizadas.

Por otra parte, Garro (comunicación personal, 7 de febrero de 2024) argumenta que actualmente el volumen de mercado costarricense no se ve tan afectado por no tener una decisión de adecuación porque:

> (...) todavía la normativa estadounidense no está exigiendo rigurosamente la aplicación del modelo europeo, pero estamos cada vez más cerca de que esto se produzca y en ese momento sí que va a ser casi que obligatorio aprobar una legislación consistente y coherente con el modelo europeo. De momento tal vez no lo estamos sintiendo mucho, pero la necesidad es latente y próximamente será evidente.

Lo anterior, cobra especial relevancia en un contexto donde EE.UU es el principal socio comercial de Costa Rica. Además, como se demostró en el capítulo anterior, EE.UU se ha visto en la necesidad de ajustarse a la normativa europea para no perder acceso a ese mercado. El año pasado, este país recibió una nueva decisión de adecuación, lo que resalta la urgencia para Costa Rica de adaptarse si no quiere enfrentar mayores implicaciones comerciales en el futuro cercano.

4.2. Mecanismos alternativos para la transferencia internacional de datos personales

La UE reconoce que "(...) no existe un planteamiento único con respecto a las transferencias internacionales de datos" (Comisión Europea, 2017, p. 11). Por lo que, si un país no logra una decisión de adecuación, las transferencias internacionales de datos personales pueden llevarse a cabo a través de instrumentos alternativos que ofrezcan garantías adecuadas en materia de protección de datos (artículo 46 del RGPD 2016). Dentro de los mecanismos se encuentran:

a. Las cláusulas contractuales tipo (CCT): son uno de los instrumentos utilizados para realizar transferencias internacionales de datos entre un país del EEE y un tercer país. Estas cláusulas estandarizadas y pre-aprobadas fueron creadas por la Comisión Europea con el fin de proporcionar un marco legal que cumpla con los requisitos del RGPD. Por ejemplo, si una empresa belga contrata la prestación de un servicio con una empresa que tiene la sede en Costa Rica, para poder realizar una transferencia de datos personales, la empresa belga (responsable del tratamiento) debe incluir en el contrato las CCT. De acuerdo con la Red Iberoamericana de Protección de Datos (s.f.), las CCT "(...) son un instrumento listo para usar y listo para ejecutar. Esto es particularmente

importante para las pequeñas y medianas empresas que no pueden permitirse otras opciones más costosas y que requieren más tiempo de implementación" (p. 17).

b. Las normas corporativas vinculantes (NCV): son las políticas de protección de datos que se asumen por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias de datos personales a un responsable o encargado que se encuentra en uno o más países terceros, ya sea dentro de un grupo empresarial o una unión de empresas que se dediquen a una actividad económica conjunta (Agencia Española de Protección de Datos, 2023). Las empresas deben presentar las NCV para su aprobación a la autoridad de protección de datos competente en la UE. En el artículo 47 apartado 2 del RGPD se establecen los elementos mínimos que deben especificar las NCV. Por otra parte, las NCV, son una buena opción para empresas multinacionales que efectúan frecuentemente transferencias de datos personales entre diferentes países.

c. Los códigos de conducta: constituyen un mecanismo de autorregulación que debe facilitar el cumplimiento del RGPD al servir como herramienta para que los responsables o encargados del tratamiento demuestren su cumplimiento. Son elaborados y adoptados voluntariamente por entidades (empresas, entidades públicas o asociaciones) que compartan una misma actividad. Los códigos de conducta son aprobados por la autoridad de control competente y tienen como fin que las entidades de un mismo sector puedan adoptar y aplicar las obligaciones del RGPD en materia de transferencia internacional de datos de acuerdo al tratamiento de datos personales que llevan a cabo (Grupo Atico34).

d. Los mecanismos de certificación: sirven para demostrar el cumplimiento de la normativa, incluyendo las garantías necesarias para las transferencias internacionales de datos. Estas certificaciones son voluntarias y están disponibles a través de un proceso ofrecido por organismos de certificación por un período máximo de tres años. Los criterios de certificación (Grupo Adaptalia, 2023).

El objetivo de estos mecanismos es permitir las transferencias internacionales de datos, garantizando que "(...) cuando se transfieran datos personales de ciudadanos europeos a terceros países, se mantenga el mismo nivel de protección con respecto a los mismos" (Comisión Europea, 2017, p. 4). Es así como, estos instrumentos proporcionan una serie de

opciones que se adaptan a distintos contextos, desde empresas multinacionales hasta pequeñas y medianas empresas, asegurando el cumplimiento de la legislación de protección de datos.

4.3. Reflexiones del capítulo

a. El RGPD ha marcado un antes y un después en las prácticas de transferencia internacional de datos a nivel global. Numerosos países consideran a la UE como un referente en materia de protección de datos personales y han adaptado su legislación para cumplir con los estándares del RGPD, asegurando así la continuidad de sus operaciones comerciales con Europa. Sin embargo, una crítica hacia este marco regulatorio es que puede percibirse como una barrera al comercio y a la inversión.

b. Entre las fortalezas del enfoque europeo respecto al intercambio transfronterizo de datos destaca su orientación centrada en las personas, así como su capacidad para simplificar dicho intercambio entre sus Estados miembros y aquellos que se ajustan a sus normativas. No obstante, también se reconocen ciertas debilidades, como los costos asociados al cumplimiento y la complejidad que enfrentan las empresas para adaptarse a las regulaciones.

c. Las decisiones de adecuación representan uno de los mecanismos que permiten a un tercer país realizar transferencias internacionales de datos sin requerir garantías adicionales. Obtener una decisión de adecuación implica que el país en cuestión cumple con un nivel de protección equivalente al de la UE. Aquellos países que no logren obtener esta adecuación pueden enfrentar diversas implicaciones, como limitaciones en su capacidad de hacer negocios, pérdida de competitividad y la necesidad de asumir costos adicionales para implementar mecanismos alternativos de transferencia internacional de datos personales, tales como CCT, NCV, códigos de conducta o mecanismos de certificación.

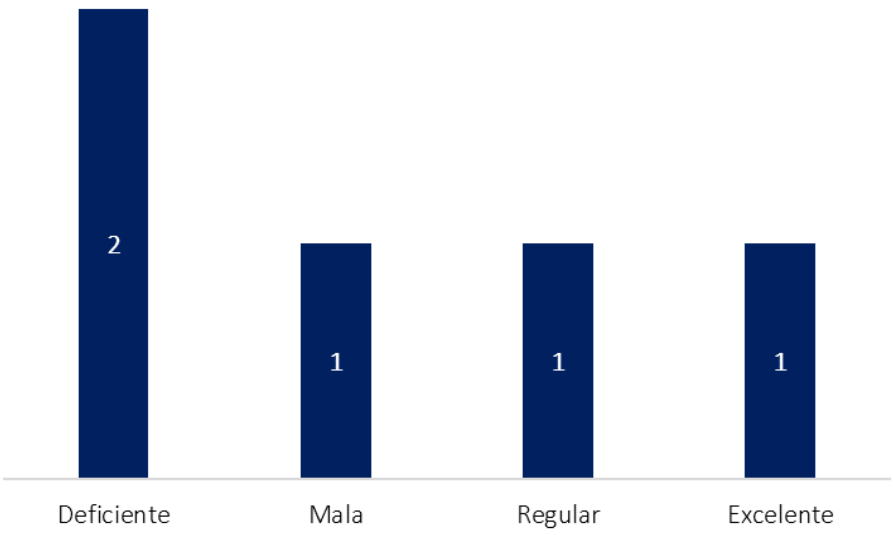
Capítulo V: Desafíos institucionales y normativos de Costa Rica en cuanto a la transferencia internacional de datos personales, recomendaciones y perspectivas globales futuras

En el presente capítulo se estudiarán los desafíos institucionales y normativos de Costa Rica en cuanto a la transferencia internacional de datos personales, recomendaciones y perspectivas globales futuras. Para ello, el capítulo se estructura de la siguiente manera: a) situación actual de Costa Rica con respecto a la transferencia internacional de datos y la normativa vigente, b) los desafíos de Costa Rica para adecuarse a la normativa europea de protección de datos personales, c) recomendaciones para Costa Rica: una futura decisión de adecuación y d) perspectivas globales venideras para la transferencia internacional de datos personales. Para alcanzar este objetivo, se toma como referencia la información recopilada a través de las entrevistas.

5.1. Situación actual de Costa Rica con respecto a la transferencia internacional de datos y la normativa vigente

Como se abordó en el capítulo III, Costa Rica, en materia de protección de datos personales, cuenta desde el 2011 con la Ley de Protección de la Persona frente al tratamiento de sus datos personales, No. 8968. Para conocer la situación actual del país en este tema, se consultó a los entrevistados su valoración (deficiente, mala, regular, excelente) sobre la normativa vigente. Los resultados obtenidos, se muestran en el gráfico 1.

Figura 11. Valoración de la situación actual de Costa Rica respecto a la transferencia internacional de datos personales y la normativa vigente



Fuente: elaboración propia con información tomada de las entrevistas realizadas.

Dos de los entrevistados valoraron la situación actual del país como deficiente, esto porque a pesar de que en Costa Rica existe la Ley No. 8968, no contiene ningún capítulo específico sobre el flujo transfronterizo de datos personales. Al respecto, Garro (comunicación personal, 7 de febrero de 2024) señala que no se incorporó este capítulo por una razón económica, que afectó no sólo a Costa Rica, sino también a los primeros países de la región que optaron por un modelo regulatorio con base en la norma europea (Argentina, Uruguay, Colombia, México, Perú)[36]. Estos países fueron reticentes a adoptar medidas sobre las regulaciones de las transferencias internacionales de datos personales debido a que las economías latinoamericanas son dependientes en gran medida de la inversión extranjera.

En este sentido, es importante comprender que la legislación de EE.UU ha contemplado históricamente los datos personales como un tema que se regula sobre la base del derecho de consumo; por su parte, la UE concibe a los datos personales como un derecho fundamental. En consecuencia, los flujos transfronterizos no habían sido un objeto regulatorio en EE.UU, por lo que, para países como Costa Rica que tienen a Estados Unidos como uno de sus principales socios comerciales, era necesario mantener esa relación económica. Por ello, en aquel momento generar un marco regulatorio con una gran influencia europea era un riesgo.

Aunado a lo anterior, uno de los entrevistados indica que la normativa de Costa Rica es mala, ya que con el paso del tiempo la Ley ha ido quedando desfasada, tomando en cuenta los fenómenos de la era digital que no fueron contemplados en su creación. Por otra parte, uno de los entrevistados menciona que la situación del país es regular y el otro entrevistado indica que es excelente; ambos dan esa valoración debido a que existe legislación en materia de protección de datos personales. No obstante, señalan que a pesar de contar con normativa, la capacidad institucional para hacer valer la legislación es el principal problema.

5.2. Los desafíos de Costa Rica para adecuarse a la normativa europea de protección de datos personales

En el capítulo IV, se discutieron las repercusiones más relevantes que enfrentan los países que no se adecuan a la normativa europea en materia de protección de datos. Para que Costa Rica aspire a cumplir con los estándares establecidos por la UE, se encuentra ante una serie de desafíos que abarcan tanto aspectos legales como técnicos y organizativos. Los

[36] En el caso de Argentina y Uruguay, la Comisión Europea les aprobó un modelo que si bien no es exacto al europeo, es paralelo. Estos dos casos son abordados en el capítulo III de este trabajo.

principales obstáculos que enfrenta Costa Rica en este proceso se presentan de manera clara en la figura 12:

Figura 12. Desafíos de Costa Rica para adecuarse a la normativa europea

Fuente: elaboración propia con información tomada de las entrevistas realizadas.

Las entrevistas realizadas revelaron que uno de los desafíos más prominentes en Costa Rica es la falta de voluntad política, especialmente en relación con las necesidades comerciales del país. De acuerdo con Garro (comunicación personal, 7 de febrero de 2024) “Si nos podemos a ver, las necesidades de desarrollar el comercio internacional por vía de la inversión extranjera son tanto la mayor motivante como la mayor limitación que tenemos para implementar un modelo adecuado a la UE”. Lemaitre (comunicación personal, 6 de marzo de 2024) argumenta que llegar a un acuerdo que permita presentar un proyecto de ley actualizado en protección de datos, que sea adecuado y que se ajuste al RGPD implica poner de acuerdo a muchos actores en materia de protección de datos (gobierno, sector privado, academia y ciudadanía).

Por otra parte, un obstáculo que se vincula con la voluntad política es el fortalecimiento de la legislación, ya que tal y como menciona Ross (comunicación personal, 1 de marzo de 2024) “(...) el actual Congreso tiene otro tipo de enfoque y tal vez el tema de la privacidad de datos no les interesa, aunque podría ser beneficioso en materia económica”. Al respecto Durán (comunicación personal, 7 de febrero de 2024) reconoce que una reforma integral a la Ley No.

8968 no iba a pasar por voluntad política y por esa razón ha optado por fragmentar la reforma en proyectos de ley pequeños. Además, aunque la necesidad de una reforma es latente; es igual de importante, que el órgano que ejerce la supervisión y la aplicación de la norma sea competente. De lo contrario, la ejecución efectiva de la legislación se verá comprometida.

Es así como sobresale la capacidad institucional débil de la Prodhab, entidad adscrita al Ministerio de Justicia y Paz, la cual carece de autonomía en sus funciones. El funcionario entrevistado de COMEX (comunicación personal, 28 de febrero de 2024) ilustra la incapacidad de la Prodhab con un ejemplo concreto: una empresa con una presencia muy importante en Costa Rica quería vender servicios que implicaban la transferencia de datos ida y vuelta entre Costa Rica y la UE. Al efectuar las gestiones correspondientes, se encontró con dos retos que impidieron gestar la homologación: a) la capacidad institucional limitada de la Prodhab y b) la falta de resoluciones por parte de la Prodhab para verificar el comportamiento de la Agencia cuando existían problemas en la protección de datos. En este contexto, uno de los principales desafíos que enfrenta Costa Rica radica en generar confianza respecto a la capacidad de la Agencia para actuar y proteger a los ciudadanos europeos cuyos datos puedan verse comprometidos en Costa Rica debido a transferencias internacionales.

Otro de los desafíos latentes en Costa Rica, es la educación y concienciación ciudadana. Tal y como afirma Durán (comunicación personal, 7 de febrero de 2024), la norma no es tan legible para el ciudadano, quién, al fin y al cabo, es el titular de los datos. Un ejemplo muy simple que evidencia el desconocimiento de las personas, es que muchas piensan que su número de cédula es un dato sensible. Esta falta de conocimiento colectiva, se refleja en la escasa comprensión de los procedimientos, la legislación, la gestión de los datos y, en última instancia, sobre sus propios derechos. Por lo tanto, incluso si la ley se reforma integralmente, si la ciudadanía no comprende la importancia de este tema, la normativa quedará en el papel, ya que ¿cómo podrán hacer valer sus derechos aquellos que ni siquiera los conocen? Al respecto, Lemaitre (comunicación personal, 6 de marzo de 2024) señala que:

> Si las personas comprendieran la magnitud de las consecuencias derivadas del mal uso de sus datos, posiblemente estarían aplicando la normativa, estarían pidiendo acciones y no solo en ciertos momentos que el tema tiene algún revuelo, como en el caso UPAD. Nadie se preocupa mucho de sus datos hasta que le pasa algo. En consecuencia, muchas veces podemos estar facilitando a empresas que no cumplen con la normativa, porque ni siquiera revisamos qué estamos haciendo.

Aunado a lo anterior, las empresas e instituciones enfrentan un desafío significativo, independientemente del sector al que pertenezcan. Los profesionales de tecnologías de la información están familiarizados con ciertas prácticas de gestión de datos. Sin embargo, la adaptación a los nuevos estándares de protección de datos puede requerir una reingeniería de procesos y un aprendizaje en cuanto a cómo manejar los datos, lo cual implica un cambio cultural y cierta complejidad. Según Lemaitre (comunicación personal, 6 de marzo de 2024), este desafío se ejemplifica en sus interacciones con empresas que buscan cumplir con las regulaciones de protección de datos. Al plantear la pregunta inicial sobre el tipo de datos que manejan, muchas de estas empresas no tienen una comprensión clara de qué tipo de datos personales están tratando. Este desconocimiento dificulta la capacidad de gestionarlos adecuadamente y subraya la necesidad de una mayor capacitación en este ámbito.

5.3. Recomendaciones para Costa Rica: una futura decisión de adecuación

En el contexto de la creciente importancia de la protección de datos a nivel global, la necesidad de Costa Rica de efectuar reformas y cambiar el paradigma en esta temática se vuelve cada vez más evidente. Por lo tanto, algunas recomendaciones que podrían orientar al país en este proceso son:

a. Fortalecer a la autoridad de protección de datos: en el caso de Costa Rica, la Prodhab. En primer lugar, es imperativo que la Prodhab no esté subordinada a ningún ministerio, incluido el Ministerio de Justicia y Paz. Esta independencia administrativa, técnica y financiera es fundamental para asegurar que la entidad pueda desempeñar sus funciones de manera imparcial y efectiva. Además, se debe dotar a la Prodhab de recursos adecuados y personal capacitado para llevar a cabo sus tareas de supervisión y aplicación de la normativa de protección de datos de manera rigurosa y eficiente. Asimismo, es necesario establecer mecanismos claros de rendición de cuentas y transparencia para garantizar la confianza pública en la labor de la Prodhab. Estas medidas fortalecerán la capacidad del país para proteger los derechos de privacidad de sus ciudadanos y promover un entorno seguro para el manejo de datos personales en todos los sectores.

b. Efectuar una reforma integral a la Ley No. 8968: en la actualidad, esta legislación carece de un capítulo específico que regule las transferencias internacionales de datos personales. En este sentido, la inclusión de disposiciones claras sobre este tema es fundamental para garantizar la adecuada protección de datos de los ciudadanos.

Además, esta reforma debería abordar otros aspectos clave, como la actualización de los principios de protección de datos para alinearse con estándares internacionales, la ampliación de los derechos de las personas y el fortalecimiento de los mecanismos de supervisión y cumplimiento. Para llevar a cabo esta reforma de manera efectiva, es necesario generar voluntad política desde un enfoque responsable. Es crucial comprender que el derecho a la protección de datos personales es inherente a la persona, y que en la era digital, donde los datos son considerados el nuevo petróleo del siglo XXI, se debe ejercer un cuidado excepcional para evitar su uso indebido, lo que podría poner en riesgo la privacidad y seguridad de los ciudadanos.

c. Concienciación en las empresas, instituciones y ciudadanía: uno de los desafíos evidenciados en el país es la falta de conocimiento, lo que se traduce en una comprensión limitada de los procedimientos, la legislación y la gestión de los datos. Por ello, resulta vital fomentar la educación y la concienciación en las empresas, instituciones y ciudadanos sobre este tema. Además, es fundamental que los ciudadanos conozcan sus derechos de protección de datos personales y comprendan cómo ejercerlos de forma correcta. Si este tema no se aborda adecuadamente, las implicaciones de no fortalecer la estructura institucional, de no llevar a cabo una reforma integral y de no lograr una decisión de adecuación podrían ser significativas. Esto podría cerrar las puertas a Costa Rica en términos de participación en mercados internacionales y dejaría al país rezagado en comparación con otros que sí están avanzando en la implementación de reformas en este ámbito. Por lo tanto, es fundamental que todos los actores involucrados comprendan su rol y estén comprometidos a realizar acciones necesarias para garantizar la adecuada protección y gestión de los datos.

5.4. Perspectivas globales venideras para la transferencia internacional de datos personales

Con el avance de las tecnologías y la expansión global de las operaciones empresariales, la transferencia de datos está experimentando un crecimiento exponencial. Esta tendencia plantea la necesidad apremiante de examinar las perspectivas globales futuras para la transferencia de datos personales. En este contexto, Garro (comunicación personal, 7 de febrero de 2024) sostiene que, debido a las constantes y significativas vulneraciones de las bases de datos, así como los daños masivos resultantes de estas violaciones, a mediano plazo se requiere

una norma supranacional, más allá del RGPD, que actualmente es el que está funcionando como tal, en ausencia de una normativa global.

Adicionalmente, según el funcionario de COMEX (comunicación personal, 28 de febrero de 2024), en la próxima reunión ministerial que se llevará a cabo en mayo de este año en la OCDE, Japón, en su rol de presidente, tiene la intención de proponer la formación de un grupo de trabajo que se encargaría de elaborar un estándar global sobre el flujo transfronterizo de datos, proporcionado por la OCDE, y buscaría llegar a un consenso entre los distintos modelos ya existentes. En este sentido, el entrevistado anticipa que el futuro en relación con este tema se vivirá en la OCDE y espera que este proceso sea una discusión sensible pero colaborativa entre los países de menor tamaño y aquellos que tienen un mayor peso en la toma de decisiones.

En conclusión, el panorama futuro de la transferencia internacional de datos se perfila desde el presente como un aspecto fundamental de la realidad digital actual. De ahí que, la necesidad de establecer un estándar internacional coherente y uniforme es más apremiante que nunca. Este estándar no solo fomentaría una mayor confianza en el intercambio de datos a escala global, lo que facilitiaría el comercio, sino que también desempeñaría un papel crucial en la protección de los derechos individuales en un entorno cada vez más digitalizado. Por ello, resulta imperativo que los países trabajen en conjunto para promover y garantizar un marco legal sólido que aborde los desafíos y oportunidades que surgen en este contexto en constante evolución. De esta manera, el futuro de la transferencia de datos se vislumbra más transparente y seguro, asegurando los derechos de las personas en todo el mundo.

5.5. Reflexiones del capítulo

a. Uno de los principales desafíos que enfrenta Costa Rica es la falta de voluntad política, ya que en la actualidad la protección de datos personales no se considera una prioridad en el Congreso. Es así como, esta falta de enfoque ha impedido la reforma de la legislación actual, la cual carece de disposiciones sobre la transferencia internacional de datos personales. Además, se destaca la limitada capacidad de la Prodhab, que forma parte del Ministerio de Justicia y Paz, carece de autonomía y cuenta con recursos y personal limitado. Por último, persiste un desafío significativo en términos de educación y concienciación ciudadana y empresarial, ya que el desconocimiento generalizado obstaculiza la implementación de acciones para promover reformas en este ámbito.

b. Para lograr un cambio de paradigma y promover reformas significativas, se recomienda fortalecer la autoridad de protección de datos, la Prodhab, otorgándole independencia administrativa, técnica y financiera, así como proporcionarle los recursos necesarios y personal capacitado. Asimismo, se sugiere llevar a cabo una reforma integral de la Ley No. 8968 para alinearla con los estándares internacionales y fortalecer los mecanismos de supervisión y cumplimiento. Por último, se propone educar a empresas, instituciones y ciudadanos para que puedan tomar acciones que fortalezcan la protección de datos en el país, asegurando que cada uno comprenda su papel en la gestión y protección de los datos.

c. Las perspectivas globales futuras para la transferencia internacional de datos personales sugieren la creación de una normativa supranacional que regule la protección y el flujo transfronterizo de datos. Esta normativa proporcionaría un estándar internacional uniforme que fortalecería la confianza en el intercambio de datos y promovería el comercio.

Conclusiones

El crecimiento exponencial de la economía de datos ha llevado a que estos sean considerados como el petróleo del siglo XXI. En este contexto, el acceso y manejo de datos personales se ha vuelto crucial para el desarrollo empresarial y económico, generando nuevas oportunidades de negocio y crecimiento. En este sentido, el marco legal internacional, en particular el RGPD de la UE, establece estándares significativos para la protección de datos personales y regula la transferencia internacional de los mismos, ya sea a través de una decisión de adecuación o de mecanismos alternativos.

Las relaciones comerciales entre la UE y Costa Rica han experimentado un notable incremento desde la firma del AACUE. Este crecimiento ha impulsado un intercambio comercial robusto, resaltando la significativa relevancia de la UE como socio comercial clave para Costa Rica. Por ello, una decisión de adecuación podría contribuir a la facilitación del comercio no solo con la UE, sino también con otros países que se han ido adecuando y han elevado sus estándares en materia de protección. Sin embargo, la falta de una regulación efectiva y de una supervisión adecuada en Costa Rica puede significar la pérdida de oportunidades en este campo en constante expansión.

Aunque Costa Rica cuenta con legislación sobre protección de datos, carece de disposiciones específicas respecto a la transferencia internacional de datos personales. Por ello, se requiere una reforma integral que no solo aborde este vacío legal, sino que también actualice los principios de protección de datos, amplíe los derechos individuales y fortalezca los mecanismos de supervisión y cumplimiento. Por otra parte, la Prodhab necesita una reestructuración que, en primer lugar, le otorgue autonomía en sus funciones, así como los recursos y el personal necesarios para llevar a cabo su razón de ser. Además, es esencial fomentar la educación y concienciación sobre la protección de datos personales tanto en el sector privado como en el público y la sociedad civil. Únicamente, a través de la colaboración entre actores se puede construir un ecosistema digital seguro, que facilite el comercio internacional y garantice la integridad de todos los ciudadanos.

Por ello, si Costa Rica busca adecuarse a la normativa europea, debe cumplir con los criterios delimitados en el capítulo IV de este trabajo, lo cual implica establecer y hacer funcionar efectivamente una o varias autoridades de control, con carácter independiente. Además, el país también tiene que asumir compromisos internacionales como adherirse al Convenio 108 y 108+, situación que aún no se ha gestado en Costa Rica. Es así como, el país

aún tiene un largo camino por recorrer para lograr la decisión de adecuación. En este panorama, Costa Rica puede enfrentarse a diversas implicaciones, como limitaciones en su capacidad de hacer negocios y desincentivar la inversión extranjera, pérdida de competitividad y la necesidad de incurrir en costos adicionales para implementar mecanismos alternativos de transferencia internacional de datos personales, tales como CCT, NCV, códigos de conducta o mecanismos de certificación.

Anexos

Anexo 1. Entrevista

Buenos días/tardes/noches:

Los datos que se le solicitarán en esta entrevista forman parte del trabajo final de graduación de la estudiante María Paula Gamboa Quirós, quién cursa estudios de maestría en Gerencia del Comercio Internacional en el Centro Internacional de Política Económica para el Desarrollo Sostenible (CINPE). El trabajo de investigación se titula *Consideraciones Normativas sobre la Transferencia Internacional de Datos Personales entre Costa Rica y la Unión Europea.* El objetivo de esta entrevista es obtener una comprensión de los diversos aspectos relacionados con la transferencia internacional de datos personales, para la identificación de desafíos y de futuros escenarios en la materia. La información que se compile a través de esta entrevista será tratada de forma confidencial y será utilizada únicamente con fines académicos.

Los temas que se abordarán son los siguientes:

a. Conocimiento general sobre la transferencia internacional de datos personales.
b. Costa Rica: situación actual y consideraciones normativas sobre la transferencia internacional de datos personales.
c. Unión Europea: legislación y prácticas relacionadas con la transferencia internacional de datos personales.
d. Desafíos normativos e institucionales para Costa Rica y perspectivas futuras.

El tiempo estimado de esta entrevista es de 30 minutos.

¿Estaría de acuerdo en grabar la entrevista?

Finalmente, ¿podemos usar su datos personales para citarlo(a) en el documento? De no ser así, la información será anonimizada.

Al finalizar el trabajo socializaré los resultados con su persona.

Instrumento

Nombre:
Cargo:
Institución:

1. ¿Qué entiende usted por el concepto de transferencia internacional de datos personales?

2. Desde su perspectiva, ¿Cuál es la principal motivación para que los países lleven a cabo transferencias de datos personales y qué tipo de dinámicas se desarrollan?

3. ¿Tiene conocimiento sobre las medidas de privacidad que se requieren para garantizar la protección de datos personales durante una transferencia internacional?

   Sí

   No

   Si lo tiene, ¿puede mencionar las medidas de privacidad más relevantes que deberían existir en una transferencia internacional de datos personales?

4. Ahora bien, si hablamos sobre Costa Rica ¿cómo valoraría la situación actual del país con respecto a la transferencia internacional de datos personales y la normativa vigente? (excelente, regular, mala o deficiente) ¿Por qué? ¿Qué hace falta?

5. En cuanto a la Unión Europea, desde su perspectiva, podría indicarme ¿Cómo ha influido el Reglamento General de Protección de Datos (RGPD) en las prácticas de transferencia internacional de datos a nivel global?

6. De acuerdo con su conocimiento, ¿Cuáles considera que son las fortalezas y debilidades de la legislación europea relacionada con la transferencia internacional de datos personales?

7. Desde su perspectiva, ¿Cuáles son algunas implicaciones comerciales y normativas que pueden tener los países que no logran una decisión de adecuación por parte de la Unión Europea?

8. ¿Qué desafíos enfrenta Costa Rica en términos de adecuación de la normativa interna a las normativas europeas de protección de datos para facilitar estas transferencias?

9. Desde su perspectiva, ¿Cuáles son algunas recomendaciones para mejorar la situación de Costa Rica en lo que respecta a la transferencia internacional de datos personales con la Unión Europea?

10. Según su perspectiva ¿Cómo visualiza a futuro la transferencia internacional de datos personales a nivel global ?

Preguntas para entrevista

#	Tema	Pregunta	Función	¿Para qué?
1	**Conocimiento general**	¿Qué entiende usted por el concepto de transferencia internacional de datos personales?	Objetivo Esp. 1	Establecer la importancia de la transferencia internacional de datos personales
2		Desde su perspectiva, ¿Cuál es la principal motivación para que los países lleven a cabo transferencias de datos personales y qué tipo de dinámicas se desarrollan?		
3		¿Tiene conocimiento sobre las medidas de privacidad que se requieren para garantizar la protección de datos personales durante una transferencia internacional? Si lo tiene, ¿puede mencionar las medidas de privacidad más relevantes que deberían existir en una transferencia internacional de datos personales?		Reconocer las medidas de privacidad que se deben tener en cuenta cuando se transfieren datos personales
4	**Costa Rica: situación actual y considera-ciones normativas**	Ahora bien, si hablamos sobre Costa Rica ¿cómo valoraría la situación actual del país con respecto a la transferencia internacional de datos personales y su normativa? (excelente, regular, mala o deficiente) ¿Por qué? ¿Qué hace falta?	Objetivo Esp. 3	Caracterizar el marco institucional costarricense en materia de datos personales
5	**Unión Europea: legislación y prácticas relacionadas con la transferencia internacional de**	En cuanto a la Unión Europea, desde su perspectiva podría indicarme ¿Cómo ha influido el Reglamento General de Protección de Datos (RGPD) en las prácticas de transferencia internacional de datos a nivel global?	Objetivo Esp.2	Comprender las prácticas de la UE así como su marco normativo en materia de transferencia internacional de datos personales
6		De acuerdo con su conocimiento, ¿Cuáles considera que son las fortalezas y debilidades de la legislación europea relacionada con la		

	datos personales	transferencia internacional de datos personales?		
7		Desde su perspectiva, ¿Cuáles son algunas implicaciones que pueden tener los países que no logran una decisión de adecuación con la Unión Europea?		
8	**Desafíos normativos e institucionales para Costa Rica y perspectivas futuras**	¿Qué desafíos enfrenta Costa Rica en términos de adecuación de la normativa interna a las normativas europeas de protección de datos para facilitar estas transferencias? qué tipos de desafíos	Objetivo Esp.3	Conocer los desafíos normativos para Costa Rica, las recomendaciones y las perspectivas futuras en materia de transferencia internacional de datos personales
9		Desde su perspectiva, ¿Cuáles son algunas recomendaciones para mejorar la situación de Costa Rica en lo que respecta a la transferencia internacional de datos personales con la Unión Europea?		
10		Según su perspectiva ¿Qué visualiza a futuro en términos de la transferencia internacional de datos?		

Referencias bibliográficas

Aberasturi Gorriño, Unai. (2011). Movimiento internacional de datos especial referencia a la transferencia internacional de datos sanitarios. Revista de Administración Pública, 186, pp. 329-369.

Agencia de Acceso a la Información Pública [AAIP]. (2023). Resolución 94/2023. https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-94-2023-384189/texto#:~:text=La%20Instituci%C3%B3n-,La%20Agencia%20de%20Acceso%20a%20la%20Informaci%C3%B3n%20P%C3%BAblica%20(AAIP)%2C,Ministros%20del%20Poder%20Ejecutivo%20Nacional.

Agencia de Acceso a la Información Pública [AAIP]. (2023). Resolución 198/2023. https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-198-2023-391538/texto

Agencia de Protección de Datos de los Habitantes [Prodhab]. (s.f.). Misión y visión. http://prodhab.go.cr/mision/

Agencia Española de Protección de Datos. (2023). Garantías para las transferencias de datos personales a terceros países u organizaciones internacionales. https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales

Agencia Española de Protección de Datos. (s.f.). ¿Qué son los códigos de conducta? https://www.aepd.es/preguntas-frecuentes/6-transferencias-internacionales-bcr-codigos-de-conducta/3-codigos-de-conducta/FAQ-0609-que-son-los-codigos-de-conducta

Ariel, S. (2017). What Are We Talking About When We Discuss Digital Protectionism?. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3032108

Asamblea Legislativa de la República de Costa Rica. (2011). Ley de Protección de la Persona frente al tratamiento de sus datos personales. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989

Asamblea Legislativa de la República de Costa Rica. (2010). Opinión Jurídica: 076-J del 12/10/2010.

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/pronunciamiento/pro_ficha.aspx?param1=PRD&param6=1&nDictamen=16464&strTipM=T#:~:text=La%20autodeterminaci%C3%B3n%20informativa%20incluye%20el,a%20que%20esta%20informaci%C3%B3n%20sea

Asamblea Nacional Constituyente. (1949). Constitución Política de la República de Costa Rica. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=871

Banco Mundial. (2021). Creating value in the data economy: The role of competition, trade, and tax policy. https://openknowledge.worldbank.org/server/api/core/bitstreams/bfe50a31-c306-5e48-a9e7-ef6e7fa45061/content

Belli, L., Brian, A., Mendoza, J., Pallazi, P., y Remolina, N. (2023). Hacia un modelo latinoamericano de adecuación para la transferencia internacional de datos personales. https://cpdp.lat/wp-content/uploads/2023/07/doc-discusion-cpdplatam23-2.3.pdf

Casalini, F. y J. López González (2019-01-23), "Trade and Cross-Border Data Flows", OECD Trade Policy Papers, No. 220, OECD Publishing, Paris. http://dx.doi.org/10.1787/b2023a47-en

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo [UNCTAD]. (2016). Data protection regulations and international data flows: Implications for trade and development. https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf

Congreso de la Nación de Argentina. (1853). Constitución de la Nación Argentina. https://wipolex-res.wipo.int/edocs/lexdocs/laws/es/ar/ar148es.pdf

Congreso de la Nación de Argentina. (1994). Constitución de la Nación Argentina. https://www.acnur.org/fileadmin/Documentos/BDL/2001/0039.pdf

Congreso de la Nación de Argentina. (2000). Ley de Protección de los Datos Personales. https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

Congreso de la Nación de Argentina. (2016). Ley de Acceso a la Información Pública. https://www.argentina.gob.ar/normativa/nacional/ley-27275-265949/texto

Consejo de Europa. (1981). Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. https://rm.coe.int/16806c1abd

Consejo de Europa. (s.f.). Convention for the Protection of Individuals with Regard to the Processing of Personal Data (CETS 108). https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958

Consejo de Europa. (s.f.). The modernised Convention 108: novelties in a nutshell. https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8

Comisión Europea. (2017). Comunicación de la Comisión al Parlamento Europeo y al Consejo: Intercambio y protección de los datos personales en un mundo globalizado. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007&from=EN

Comisión Europea. (2020). La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0264

Comisión Europea. (2021). Protección de datos: la Comisión Europea pone en marcha el procedimiento sobre los flujos de datos personales al Reino Unido.

Comisión Europea. (2023). Informe de la Comisión al Parlamento Europeo y al Consejo sobre la primera revisión del funcionamiento de la decisión de adecuación relativa a Japón. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52023DC0275

Comisión Europea. (2023). Protección de datos: la Comisión Europea adopta una nueva decisión de adecuación para la circulación de datos UE-EE.UU. con seguridad y confianza. https://ec.europa.eu/commission/presscorner/api/files/document/print/es/ip_23_3721/IP_23_3721_ES.pdf

Comisión Europea. (s.f.). ¿Qué son los datos personales?. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_es

Comisión Europea. (s.f.). ¿Qué datos personales se consideran sensibles?. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_es

Comisión Europea (2024). Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC. https://commission.europa.eu/system/files/2024-01/JUST_template_comingsoon_Report%20on%20the%20first%20review%20of%20the%20functioning.pdf

Cordero, C. (2019). La transferencia internacional de datos con terceros Estados en el nuevo Reglamento Europeo: especial referencia al caso estadounidense y la cloud act. https://revistasmarcialpons.es/revistaespanoladerechoeuropeo/article/download/54/77

Deloitte. (2022). Normas relevantes en materia de datos personales del año 2021. https://www2.deloitte.com/uy/es/pages/tax/articles/normas-relevantes-en-materia-de-datos-personales-del-2021.html

Duarte. (2023). Amount of Data Created Daily (2024). https://explodingtopics.com/blog/data-generated-per-day

Gobierno de Argentina. (2024). Argentina logró la nueva adecuación por parte de la Unión Europea para el flujo internacional de datos personales. https://www.argentina.gob.ar/noticias/argentina-logro-la-nueva-adecuacion-por-parte-de-la-union-europea-para-el-flujo#:~:text=de%20datos%20personales-,Argentina%20logr%C3%B3%20la%20nueva%20adecuaci%C3%B3n%20por%20parte%20de%20la%20Uni%C3%B3n,datos%20personales%20que%20la%20UE.

Gobierno de Argentina. (2022). Impulsada por la Agencia de Acceso a la Información Pública, Argentina adhirió al Convenio 108+. https://www.argentina.gob.ar/noticias/impulsada-por-la-agencia-de-acceso-la-informacion-publica-argentina-adhirio-al-convenio-108#:~:text=En%20tanto%2C%20la%20Argentina%20es,firmar%20el%20Convenio%20108%20modernizado.

Gobierno de Argentina. (2023). La AAIP aprobó cláusulas contractuales modelo de la RIPD para transferencias internacionales de datos. https://www.argentina.gob.ar/noticias/la-aaip-aprobo-clausulas-contractuales-modelo-de-la-ripd-para-transferencias

Gobierno de Argentina. (s.f.). Nuevo Proyecto de Ley de Protección de Datos Personales. https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales

Gonzalo, J. (2019) Las decisiones de adecuación en el derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los Estados miembros. https://doi.org/10.20318/cdt.2019.4624

Grupo Adaptalia. (2023). ¿Qué es una transferencia internacional de datos? https://grupoadaptalia.es/blog/transferencia-internacional-de-datos/#_%C2%BFQue_son_los_mecanismos_de_certificacion

Grupo Atico34. (s.f.). Códigos de conducta en protección de datos ¿Qué son? https://protecciondatos-lopd.com/empresas/codigo-conducta/#:~:text=Los%20c%C3%B3digos%20de%20conducta%20en%20protecci%C3%B3n%20de%20datos%20son%20un,actividad%20que%20desarrollan%20y%20los

Grupo de Trabajo del artículo 29 [GT29]. (2016). Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision. https://ec.europa.eu/newsroom/article29/items/640157

IBM Security. (2019). Por qué es importante la privacidad de los datos. https://www.ibm.com/downloads/cas/AKL1VJ6O

Matus, J. (2010). Transferencias internacionales a países con niveles adecuados y no adecuados de protección: aspectos prácticos. https://www.redipd.org/sites/default/files/2020-01/Ponencia_J_Matus.pdf

Oficina Económica y Comercial de España en Panamá. (2022). Informe Económico y Comercial: Costa Rica. https://www.icex.es/content/dam/es/icex/documentos/quienes-somos/donde-estamos/red-exterior/costa-rica/DOC2022910448.pdf

Organización de las Naciones Unidas [ONU]. (1948). La Declaración Universal de los Derechos Humanos. https://www.un.org/es/about-us/universal-declaration-of-human-rights +

Organización de los Estados Americanos [OEA]. (2021). Principios actualizados sobre la privacidad y la protección de datos personales. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Organización Mundial del Comercio [OMC]. (2018). Los principios del sistema de comercio. https://www.wto.org/spanish/thewto_s/whatis_s/tif_s/fact2_s.htm#:~:text=Trato%20nacional%3A%20igual%20trato%20para,hayan%20entrado%20en%20el%20mercado.

Organización Mundial del Comercio [OMC]. (s.f.). ¿Cómo prepararse para la transformación del comercio asociada a la tecnología? https://www.wto.org/spanish/res_s/publications_s/wtr18_4_s.pdf

Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2022). Catalizadores digitales de la economía mundial: documento de referencia para la Conferencia Ministerial del CDEP. https://www.oecd-ilibrary.org/docserver/eaf5082e-es.pdf?expires=1708997224&id=id&accname=guest&checksum=E0E8A9CB57D4899667D2627FAF4046B3

Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2002). Resumen: directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. https://www.oecd.org/sti/ieconomy/15590267.pdf

Pacto Mundial de las Naciones Unidas. (2022). ¿Qué son los derechos digitales y cuál es su relación con los ODS?. https://www.pactomundial.org/noticia/que-son-los-derechos-digitales-y-cual-es-su-relacion-con-los-ods/

París, M. (2020). Constitucionalización del derecho a la protección de datos. *Delfino.* https://delfino.cr/2020/03/constitucionalizacion-del-derecho-a-la-proteccion-de-datos

Parlamento del Uruguay. (2008). Ley de Protección de Datos Personales. https://www.impo.com.uy/bases/leyes/18331-2008

Parlamento Europeo. La Protección de los Datos Personales. https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/es/FTU_4.2.8.pdf

Parlamento y Consejo Europeo. (1995). Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta el tratamiento de datos personales y a la libre circulación de estos datos. https://www.boe.es/doue/1995/281/L00031-00050.pdf

Parlamento y Consejo Europeo. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). https://www.boe.es/doue/2016/119/L00001-00088.pdf

Polo, A. (2021). Las transferencias internacionales de datos: regulación actual y su incidencia en las relaciones exteriores de la Unión Europea. https://dialnet.unirioja.es/descarga/articulo/8147963.pdf

Ramírez, A. (2023). 4 razones para reformar la Ley de Protección de Datos Personales. *CRHoy*. https://www.crhoy.com/nacionales/4-razones-para-reformar-la-ley-de-proteccion-de-datos-personales/

Red Iberoamericana de Protección de Datos. (2017). Estándares de Protección de Datos Personales. https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

Red Iberoamericana de Protección de Datos. (s.f.). Guía de implementación: cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP). https://www.redipd.org/sites/default/files/2023-02/guia-implementacion-clausulas-contractuales-modelo-tidp-es.pdf

Recio Gayo, M. (2019). Nivel adecuado para transferencias internacionales de datos. Derecho PUCP, (83), 207 - 240. https://doi.org/10.18800/derechopucp.201902.007

Sampieri, R. (2018). Metodología de la investigación. https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Schwartz, P. (2004). Property, Privacy, and Personal Data. Harvard Law Review, 117(7), 2056–2128. https://doi.org/10.2307/4093335

Sobrino, I. (2021). Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Estados Unidos. https://www.researchgate.net/publication/351097683_Las_decisiones_de_adecuacion_en_las_transferencias_internacionales_de_datos_El_caso_del_flujo_de_datos_entre_la_Union_Europea_y_Estados_Unidos

Wu, Tim (2006) "The World Trade Law of Censorship and Internet Filtering," Chicago Journal of International Law: Vol. 7: No. 1, Article 12. https://chicagounbound.uchicago.edu/cjil/vol7/iss1/12

Yakovleva, S. (2022). Personal data transfers in international trade and EU law: a tale of two necessities. The Journal of World Investment & Trade, 21(6), 881-919. doi: https://doi.org/10.1163/22119000-12340189

Zorraquino, A., Vilanova, R., y Betorz, A. (2023). EU-U.S. Data Privacy Framework: Nuevo escenario para las transferencias internacionales de datos personales a los Estados Unidos. https://periscopiofiscalylegal.pwc.es/wp-content/uploads/2023/07/EU-U.S.-Data-Privacy-Framework-Nuevo-escenario-para-las-transferencias-internacionales-de-datos-personales-a-los-Estados-Unidos-2.pdf