https://doi.org/10.18800/derechopucp.201902.007

DERECHO PUCP
N° 83, 2019
diciembre-mayo
pp. 207-240
REVISTA DE LA FACULTAD DE DERECHO

Nivel adecuado para transferencias internacionales de datos

Adequate Level for International Data Transfers

MIGUEL RECIO GAYO*
Universidad CEU San Pablo (Brasil)

Resumen: Como concepto, el de nivel adecuado de protección para las transferencias internacionales de datos sigue siendo, en cierta medida, desconocido. En el caso de la Unión Europea, con respecto a la directiva 95/46/CE, ya derogada, su contenido ha sido concretado por el Reglamento General de Protección de Datos (RGPD). Su origen está, en la era predigital, en instrumentos internacionales sobre protección de datos personales. Su desarrollo más relevante se ha producido en la Unión Europea, hasta llegar al caso de la decisión de adecuación de Japón —la primera adoptada después del 25 de mayo de 2018, en la que puede verse la aplicación práctica de los elementos que se requieren conforme al RGPD—. Otros países, en particular en América Latina, también han incluido en sus leyes sobre protección de datos el concepto de nivel adecuado. A pesar de que el nivel adecuado es solo uno de los instrumentos para las transferencias internacionales de datos, las diferencias que pueden surgir, entre países o regiones, en cuanto a qué países tienen o no un nivel adecuado de protección para la transferencia internacional de datos, podrían dar lugar a considerar si sería aconsejable un estándar multilateral que facilitara esta última. En cualquier caso, debe considerarse también que el modelo de adecuación es uno de los instrumentos para la transferencia internacional de datos, pero no el único, ya que pueden existir otros mecanismos para aplicar protecciones adecuadas y efectivas en materia de protección de datos.

Palabras clave: protección de datos personales, derechos fundamentales, transferencia internacional de datos, nivel adecuado, Reglamento General de Protección de Datos, Comisión Europea, decisión de adecuación, economía digital

Abstract: As a concept, the adequate level of protection for international data transfers remains to some extent unknown and, in the case of the European Union, with regard to Directive 95/46/EC, already repealed, its content has been specified by the General Data Protection Regulation (GDPR). Its origin is, in the pre-digital era, in international instruments on the protection of personal data and its most relevant development has occurred in the European Union, until reaching the case of the adequacy decision of Japan, which is the first adopted after 25 of May of 2018, which shows the practical application of the elements required under the GDPR. Other countries, particularly in Latin America, have also included the concept of

* Doctor en Derecho. Máster en Protección de Datos, Transparencia y Acceso a la Información por la Universidad San Pablo CEU (Madrid) y máster en Derecho de la Propiedad Intelectual por The George Washington University Law School (Washington D.C.). Abogado radicado en Madrid (España).
Código ORCID: 0000-0002-2282-9907. Correo electrónico: miguelrecio@miguelrecio.com

adequate level in their data protection laws. Although the adequate level is only one of the instruments for international data transfers, the differences that may arise, between countries or regions, as to which countries have an adequate level of protection for international data transfer could lead to consider whether a multilateral standard that facilitates the latter is advisable. In any case, it should also be considered that the adequacy model is one of the instruments for the international transfer of data, but not the only one, since there may be other mechanisms to apply adequate and effective data protection protections.

Key words: personal data protection, fundamental rights, international data transfer, adequate level, General Data Protection Regulation, European Commission, adequacy decision, digital economy.

I. INTRODUCCIÓN

El nivel adecuado de protección de datos para las transferencias internacionales de datos es un concepto relevante, pero en cierta medida desconocido. Desde la década de 1980, todavía en una era predigital, cuando se publicaron los primeros instrumentos internacionales en materia de protección de datos, todo ha cambiado de manera vertiginosa. Ya en estos instrumentos se incluían referencias a las garantías adecuadas para la transferencia internacional de datos: en ellos se señalaba claramente que debía garantizarse el libre flujo internacional de datos.

Actualmente, cuando el mundo está interconectado gracias a Internet y la «digitalización de todo» (Parlamento Europeo, 2016, p. 4), son necesarias aproximaciones apropiadas que faciliten que la sociedad y la persona se beneficien de la innovación tecnológica y que permitan avanzar en el desarrollo de una economía digital robusta y próspera. Al respecto, los flujos, movimientos o transferencias internacionales de datos personales son esenciales para poder lograr dichos objetivos. La posibilidad de utilizar servicios como la computación en la nube (en inglés, *cloud computing*), el tratamiento analítico de datos masivos (en inglés, *big data analytics*) o la inteligencia artificial, además de la posibilidad de acceder a otros servicios proporcionados por proveedores de servicios o emprendedores establecidos en otros países alrededor del mundo, requieren de aproximaciones integrales —que consideren todos los aspectos que se plantean— y multilaterales —que incluyan a todas las partes—.

Una cuestión necesaria para que las transacciones —económicas o no, públicas o privadas— sean factibles y para poder garantizar derechos tales como la libertad de expresión o el acceso a la información pública es que las transferencias internacionales de datos deben ser objeto de una cooperación responsable que supere aproximaciones unilaterales o parciales. Además, existen límites claros al adoptar medidas, ya que el artículo XIV del Acuerdo General sobre el Comercio de Servicios de la Organización Mundial del Comercio (OMC), partiendo de la salvaguardia de la protección de datos personales, prevé que las medidas que adopten los países al respecto no puedan dar lugar ni a una discriminación arbitraria o injustificable cuando existan condiciones similares, aunque no idénticas, ni a una restricción encubierta del comercio de servicios.

El nivel adecuado de protección para la transferencia internacional de datos desempeña un importante papel para lograr los objetivos de una sociedad y una economía digitales inclusivas y prósperas. Esto implica que resulte conveniente conocer el origen del concepto y el modo en el que ha evolucionado —considerando, en particular, el prominente desarrollo del concepto en el ámbito de la Unión Europea y la manera en que otros países alrededor del mundo se han aproximado a este concepto—.

El mosaico al que da lugar la aproximación unilateral al concepto de nivel adecuado de protección para las transferencias internacionales de datos lleva a plantear si resultaría conveniente un estándar multilateral que sea resultado del consenso más amplio posible sobre este concepto. Por último, se incluyen en el artículo las conclusiones a las que da lugar el análisis hecho a lo largo del mismo.

II. REFERENCIAS EN INSTRUMENTOS INTERNACIONALES AL TÉRMINO NIVEL ADECUADO PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS

II.1. Directrices de la OCDE de 1980 y de 2013

El recurso al nivel adecuado, como criterio a considerar en el caso de las transferencias internacionales de datos, surge a partir de las previsiones en instrumentos internacionales. En concreto, el primero de estos instrumentos fue las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales, adoptadas en virtud de una Recomendación del Consejo el 23 de setiembre de 1980.

En aquel momento, a finales del siglo pasado, las transferencias internacionales de datos se caracterizaban por transmisiones punto a punto entre empresas o gobiernos. Desde entonces, el entorno ha cambiado sustancialmente, ya que actualmente la tecnología permite un tratamiento simultáneo de cantidades masivas de datos que pueden ser transmitidos a múltiples destinatarios; datos que pueden ser almacenados en centros de datos alrededor del mundo y a los que puede accederse desde cualquier lugar en el que alguien pueda conectarse a Internet.

La parte tercera de las Directrices incluía los principios básicos en materia de flujo o transferencia internacional de datos personales. Al respecto, cabe destacar que el título de esta parte de las Directrices era el de libre flujo y restricciones legítimas. La norma general, según el numeral 16 de las Directrices, era que los países miembros debían adoptar todas las medidas adecuadas para asegurar que las transferencias internacionales de datos personales, incluyendo el tránsito a través de otro país parte, fueran ininterrumpidas y seguras. Es decir, los flujos internacionales de datos deberían ser admitidos cuando los requisitos de las Directrices hubieran sido cumplidos sustancialmente, es decir, de manera efectiva (OCDE, 2013, p. 60).

Al respecto, las Directrices preveían, respectivamente en los numerales 17 y 18, dos límites para asegurar que los países parte de la OCDE no estableciesen restricciones indebidas al libre flujo internacional de los datos personales. El primero era que, como norma general, los países parte no deberían restringir las transferencias internacionales, salvo cuando el otro país parte no observara todavía sustancialmente las Directrices o las transferencias ulteriores —es decir, cuando la reexportación de los datos personales tuviera como finalidad eludir o evadir la legislación nacional en la materia—. Un país parte podría imponer restricciones en el caso de ciertas categorías de datos personales para las que la legislación del país de origen incluyera una regulación específica en virtud de la naturaleza de los datos personales y cuando el país de destino no tuviera

una protección equivalente (en inglés, *equivalent protection*). El segundo límite era que los países parte tendrían que evitar adoptar leyes, políticas y prácticas basadas en la protección de la privacidad y de las libertades individuales que pudieran crear obstáculos o barreras a las transferencias internacionales de datos cuando excedieran los requisitos de protección.

Es importante tener en cuenta que el numeral 17 utilizaba el término protección equivalente —según la traducción del original, en inglés, *equivalent protection*—, término que puede considerarse como similar al de nivel adecuado. No obstante, ambos términos, aunque aquí se usan indistintamente, podrían tener un significado diferente. En efecto, (OECD, 2018, p. 20) mientras que la equivalencia implica la evaluación de un nivel de similitud objetiva entre dos marcos, considerando los instrumentos utilizados y los resultados de la regulación; la adecuación puede ser más flexible, ya que implica estar de acuerdo sobre un resultado común y permiten el uso de diferentes instrumentos para alcanzar dicho resultado.

Estas Directrices fueron revisadas y actualizadas en 2013. En particular, la necesidad de abordar la dimensión global de la protección de datos y la privacidad es una de las cuestiones relevantes que se tuvo en consideración en dicha revisión y actualización. Es así que la OCDE refleja en sus Directrices actuales los avances que se han producido durante las últimas décadas en materia de transferencias internacionales de datos. Asimismo, destaca que la existencia de garantías adecuadas, que pueden basarse en mecanismos diversos, debe dar lugar a la eliminación de restricciones.

II.2. Convenio 108 del Consejo de Europa y versión actualizada

El Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, dedica su artículo 12 a los flujos transfronterizos de datos. El párrafo segundo del citado artículo establecía la norma general de prohibición de que las partes del Convenio pudieran restringir la transferencia internacional de datos. Se trataba de una previsión similar a la del numeral 18 las Directrices de la OCDE, en la versión de 1980, por lo que se refiere a que los países parte no pueden recurrir a la protección de datos como argumento para restringir las transferencias internacionales de datos, salvo cuando existan causas o motivos legítimos.

Es decir, el Convenio 108 del Consejo de Europa preveía que la norma general de libre flujo transfronterizo de los datos personales solo podría ser objeto de restricción en dos supuestos. En virtud del párrafo tercero

del artículo 12, uno de estos supuestos era el relativo, por una parte, a determinadas categorías de datos o bases de datos sobre los que la legislación del país de origen incluyera una reglamentación específica. En este caso, se requería que la reglamentación de la otra parte estableciera una protección equivalente para que la restricción indicada no aplicase.

Y, por otra parte, también se podría restringir el flujo transfronterizo de datos cuando

> la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte (artículo 12.3.b).

No obstante, es importante considerar las cifras en lo que se refiere al número de países que eran parte de este Convenio, a efectos de discutir, por una parte, las garantías adecuadas y, por otra parte, el mecanismo europeo de nivel adecuado. Es así que el total de países parte del Convenio 108 era 54, lo que supone menos de la mitad del total de países que cuentan ya con legislación en materia de protección de datos o privacidad —si se considera que habría ya 132 países (Greenleaf, 2019)—. De estos 54 países, más de la mitad (28) son los Estados miembros de la Unión Europea y otros tres son países del Espacio Económico Europeo (Islandia, Noruega y Liechtenstein). Esto supone que más de la mitad de los países que son parte del Convenio 108, es decir, el 57,4%, son países del Espacio Económico Europeo, donde es aplicable el Reglamento General de Protección de Datos, ya que este fue incluido en el Acuerdo sobre el Espacio Económico Europeo (EEE)[1] en virtud de la decisión del Comité Mixto del EEE 154/2018, de 6 de julio de 2018, por la que se modifica el anexo XI (Comunicación electrónica, servicios audiovisuales y sociedad de la información) y el Protocolo 37 (que contiene la lista prevista en el artículo 101) del Acuerdo EEE 2018/1022.

Es decir, además de los indicados, veintitrés países parte del Convenio 108 deberían tener garantizado el libre flujo internacional de los datos en los términos previstos en el mismo. De estos, cuatro (Andorra, Argentina, Suiza y Uruguay) han obtenido una decisión de adecuación, lo que supone que el 21% de los países parte del Convenio 108 que no son países del Espacio Económico Europeo hayan optado por la declaración de nivel adecuado otorgada por la Comisión Europea. No obstante, estas cifras cambiarán próximamente con la versión actualizada del Convenio.

1 Al respecto, pueden verse los documentos contenidos en el siguiente vínculo: https://www.efta.int/eea-lex/32016R0679

El Convenio 108 fue actualizado en 2018, dando lugar al Convenio 108+. Por lo que se refiere, en particular, a las transferencias internacionales de datos cuando un país destinatario no está sujeto a la jurisdicción de una parte (Consejo de Europa, 2018, p. 5) se requiere que se garantice un nivel adecuado de protección de datos. Ello puede alcanzarse a través de diversos instrumentos, tales como las cláusulas contractuales o las normas corporativas vinculantes.

Por lo tanto, debe tenerse en cuenta que una declaración de nivel adecuado es uno de los instrumentos existentes, lo que no impide que quienes tratan datos personales puedan recurrir a otros, siempre y cuando las medidas que se adopten garanticen una protección efectiva.

III. SIGNIFICADO Y ALCANCE DEL NIVEL ADECUADO PARA TRANSFERENCIAS INTERNACIONALES DE DATOS

Atendiendo específicamente al caso de la Unión Europea, por ser donde se desarrolló en primer lugar la aproximación a las transferencias internacionales de datos basadas en el modelo de adecuación, cabe señalar que ni la directiva 95/46/CE ni el RGPD definen el concepto de nivel adecuado.

Sin perjuicio de la ausencia de una definición normativa sobre qué se entiende por nivel adecuado, el Tribunal de Justicia de la Unión Europea (TJUE) tuvo oportunidad de pronunciarse al respecto en la sentencia de 6 de octubre de 2015, en el asunto C-362/14 (*Maximillian Schrems c. Data Protection Commissioner*), en la que anuló el Acuerdo de Puerto Seguro (en inglés, *Safe Harbor Agreement*) entre la Unión Europea y los Estados Unidos de América. En concreto, el TJUE indicó al respecto que

> el término «adecuado» 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 (apartado 73).

A continuación, el TJUE indicaba también, recurriendo a las conclusiones del Abogado General para fundamentar su razonamiento, que

> 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, entendida a la luz de la Carta [de los Derechos Fundamentales de la Unión Europea] (apartado 73).

Es así que el requisito de que el tercer país tenga un nivel «esencialmente equivalente» al que se aplica en la Unión Europea es el contenido del test que estableció el TJUE en dicha sentencia. Es importante tener en cuenta al respecto que lo que se requiere a terceros países es un nivel sustancialmente equivalente, pero no igual, al que proporciona la legislación europea sobre protección de datos.

Como explica el TJUE en el apartado 72, mencionando de nuevo las conclusiones del Abogado General, de lo que se trata es de que el nivel adecuado de protección de datos permita «asegurar la continuidad del elevado nivel de protección» de datos previsto en la normativa europea. Ahora bien, 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.

IV. ¿QUÉ ES EL «MODELO DE ADECUACIÓN»?

El denominado «modelo de adecuación» (en inglés, *adequacy model*) es un mecanismo, desarrollado fundamentalmente en la Unión Europea, que tiene por finalidad asegurar la protección de las personas físicas cuando se llevan a cabo transferencias internacionales de datos personales. En concreto, consiste en realizar una evaluación específica del país al que se va a realizar la transferencia internacional de datos. Cabe señalar que existen también otros mecanismos alternativos que no están basados en la evaluación específica del país, sino en las garantías adoptadas por los responsables del tratamiento —como, por ejemplo, las cláusulas contractuales modelo (en inglés, *standard contractual clauses*, SCC); las normas corporativas vinculantes (*Binding Corporate Rules*, BCRs); las reglas transfronterizas de privacidad (*Cross-Border Privacy Rules*, CBPRs); o excepciones para situaciones específicas, tales como el consentimiento del interesado—. Este mecanismo de adecuación consiste, como lo definió el Grupo de Trabajo del Artículo 29[2], en que la Comisión Europea confirme «formalmente, con efectos vinculantes para los Estados miembros, que el nivel de protección de datos en un tercer país u organización internacional es sustancialmente equivalente al nivel de protección de datos en la Unión Europea» (Grupo de Trabajo del Artículo 29, 2018, p. 2).

También debe tenerse en cuenta que, como ha indicado la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNTACD, por sus siglas en inglés), la adecuación en protección de datos tiene ventajas e inconvenientes. Como ventajas, puede destacarse que permite la transferencia integral a los países que han recibido el nivel de adecuación

2 El Grupo de Trabajo del Artículo 29 se integró, el 25 de mayo de 2018, en el Comité Europeo de Protección de Datos (CEPD).

y que se basa en una lista transparente y abierta. Como inconveniente, cabe resaltar que se requiere un proceso largo hasta que, si procede, se reconoce el nivel adecuado del país del que se trate (UNCTAD, 2016, p. 14).

No obstante, si consideramos que alrededor de 132 países tienen actualmente legislación en materia de protección de datos —de los que habría que quitar 31, ya que son los 28 Estados miembros de la Unión Europea más los otros 3 del Espacio Económico Europeo ya indicados— (y aunque en 13 casos, incluyendo Canadá y Estados Unidos, se trate de adecuaciones parciales); es posible afirmar que menos del 13% de los denominados terceros países con respecto a la Unión Europea han obtenido una declaración de adecuación de la Comisión Europea.

Por último, si se tienen en cuenta las diferentes aproximaciones a nivel internacional, es posible notar que incluyen diferentes niveles de requisitos regulatorios. Y esto puede crear problemas, en particular en términos de costos de cumplimiento, para organizaciones que, por diferentes motivos, tratan datos personales en diversas jurisdicciones y, por tanto, quedan sujetos a regímenes diferentes (GSMA, 2018, p. 19).

V. ENFOQUE EUROPEO: DE LA DIRECTIVA 95/46/CE AL RGPD

V.1. Aproximación general al nivel adecuado para las transferencias internacionales de datos

El término nivel adecuado fue incluido, por primera vez en la Unión Europea, en el párrafo primero del artículo 25 de la directiva 95/46/CE, derogada el 24 de mayo de 2016 por la entrada en vigor del Reglamento General de Protección de Datos (en adelante, RGPD)[3].

Esta directiva, ni en sus considerandos ni en el artículo 2, relativo a las definiciones, definió qué se entendía por nivel adecuado. No obstante, en el considerando 56 explicaba que la Unión Europea «no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado». Asimismo, sostenía que el nivel adecuado «debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias».

El enfoque europeo difiere, en cierta medida, de lo previsto tanto en las Directrices de la OCDE como en el Convenio 108+ del Consejo de Europa. A pesar de que la Unión Europea no se opone a la transferencia de

3 A partir del 25 de mayo de 2018, ya que entró en vigor el 24 de mayo de 2016, a los veinte días de su publicación en el *Diario Oficial de la Unión Europea* (artículo 99 del RGPD).

datos personales a países que garanticen un nivel de protección de datos adecuado, exige que, aunque sean partes del Convenio 108, obtengan una declaración de adecuación de la Comisión Europea. Por ejemplo, aunque México haya accedido al Convenio 108, es considerado todavía un tercer país sin nivel adecuado y, por tanto, requiere de una decisión de adecuación u otra garantía adecuada para que se pueda llevar a cabo una transferencia internacional de datos desde la Unión Europea.

El RGPD, que derogó a la directiva 95/46/CE, supone un cambio con respecto a esta última por lo que se refiere a las transferencias internacionales de datos. Al respecto, la Comisión Europea ya explicaba, antes de la aplicación efectiva del RGPD, que «la reforma de las normas relativas a las transferencias internacionales aclara y simplifica su utilización e introduce nuevos instrumentos de transferencia» (Comisión Europea, 2017, p. 3).

En este sentido, aunque la decisión de adecuación de la Comisión Europea es el primero de los instrumentos que se menciona en el RGPD a efectos de poder llevar a cabo transferencias internacionales de datos a terceros países sin nivel adecuado, es necesario tener en cuenta que existen también otros instrumentos. Es decir, entre los diversos instrumentos no existe una relación de jerarquía, sino que todos, incluidas las decisiones de adecuación, son alternativos. Son tres las bases legales para la transferencia internacional de datos incluidas en la directiva 95/46/CE y mantenidas en el RGPD (Kuner, 2017, p. 904): (a) decisiones de adecuación de la Comisión Europea; (b) garantías adecuadas, debiendo entender que puede haber otras además de la decisión de adecuación; y (c) excepciones para situaciones específicas.

Esto significa que una empresa establecida en el Espacio Económico Europeo (EEE) —sin perjuicio de que se prevean también supuestos específicos para las Administraciones Públicas—, cuando vaya a transferir datos personales a un tercer país sin nivel adecuado, puede recurrir, respectivamente, a alguno de los instrumentos previstos en el RGPD. No obstante, es cierto que en algunos casos dependerá de que la Comisión Europea, o quien corresponda en cada caso, haya adoptado la medida de que se trate como, por ejemplo, la decisión de adecuación.

Sin perjuicio de lo anterior, las decisiones de adecuación de la Comisión Europea supondrían el estándar más alto (Kuner, 2017, p. 904), al requerir que el sistema legal del tercer país sea sustancialmente equivalente —según la traducción del inglés «essentially equivalent»—. Esto implica que, cuando exista una decisión de adecuación, se podrá recurrir a alguna de las otras garantías adecuadas y excepciones para situaciones específicas.

Desde la perspectiva de si requieren o no autorización expresa de una autorización expresa de la autoridad de protección de datos correspondiente, los instrumentos que no requieren de dicha autorización son los siguientes:

- Una decisión de adecuación de la Comisión Europea (artículo 45 del RGPD);
- un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos (artículo 46.2.a del RGPD);
- las normas corporativas vinculantes (artículo 46.2.b del RGPD);
- cláusulas tipo de protección de datos adoptadas por la Comisión Europea (artículo 46.2.c del RGPD)[4];
- cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión Europea (artículo 46.2.d del RGPD);
- un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados (artículo 46.2.d del RGPD); o
- un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados (artículo 46.2.d del RGPD).

Y, por otra parte, los instrumentos que sí requieren de una autorización expresa de una autoridad de protección de datos son los siguientes:

- Cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional (artículo 46.3.a del RGPD); o
- disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados (artículo 46.3.b del RGPD).

4 Actualmente, existen tres modelos de cláusulas tipo aprobados por la Comisión. Dos de estos modelos se refieren a la transferencia entre un responsable del tratamiento en el EEE y otro responsable del tratamiento establecido en un tercer país. Estos son la Decisión 2001/497/CE de la Comisión y la Decisión 2004/915/CE de la Comisión. Y el tercer modelo es el relativo a la transferencia de datos por un responsable del tratamiento establecido en el EEE a un encargado del tratamiento en un tercer país. Se trata de la Decisión 2010/87/CE de la Comisión.

Finalmente, existen también excepciones para situaciones específicas. Entre estas excepciones se encuentra, por ejemplo, el consentimiento explícito del interesado (artículo 49.1.a del RGPD). Ahora bien, estas excepciones se interpretarán, como ha indicado el Comité Europeo de Protección de Datos (CEPD), de manera restrictiva, con la finalidad de que no se conviertan en la regla general (CEPD, 2018a, p. 4).

V.2. Los elementos específicos para evaluar la adecuación del nivel de protección en el RGPD

En comparación con la directiva 95/46/CE —que, en el artículo 25.2, en términos generales, ya incluía los criterios a considerar para evaluar el «carácter adecuado del nivel de protección que ofrece un país tercero»—, en el RGPD se han detallado estos criterios. En concreto, el artículo 25.2 de la directiva 95/46/CE indicaba que el nivel adecuado de protección que ofrece un país tercero se evaluará atendiendo a

> todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Actualmente, el artículo 45.2 del RGPD incluye los elementos que, en particular, tendrá en cuenta la Comisión Europea al evaluar la adecuación del nivel de protección y que se refieren a los elementos que se exponen a continuación. El primero es el Estado de Derecho, lo que incluye la legislación, jurisprudencia, los derechos efectivos y exigibles y el acceso a la justicia por los interesados cuyos datos personales sean objeto de transferencia a un tercer país.

En concreto, el artículo 45.2.a) del RGPD indica que se evaluará

> 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.

En particular, en lo que se refiere al contenido esencial de este elemento, el derecho fundamental a la protección de datos en la Unión Europea está previsto en la Carta de los Derechos Fundamentales e implica que el tratamiento de los datos personales se lleve a cabo de modo leal, para fines concretos y sobre una base de legitimación, además de reconocer a toda persona los derechos de acceso y rectificación.

Y en cuanto al acceso a la justicia, es decir, a recursos administrativos y acciones judiciales que sean efectivos, el artículo 47 de la Carta de los Derechos Fundamentales reconoce el derecho a la tutela judicial efectiva y a un juez imparcial, lo que tiene especial relevancia cuando el citado artículo del RGPD se refiere a las acciones judiciales que sean efectivas.

El segundo de los elementos es la existencia y el funcionamiento efectivo de una o varias autoridades de protección de datos o autoridades de control independientes en el tercer país. Al respecto, el artículo 45.2.b) del RGPD indica que este elemento consiste en

> 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.

En este sentido, el artículo 8.3 de la Carta de los Derechos Fundamentales incluye como elemento esencial de la garantía del derecho fundamental a la protección de datos el control del respeto de las normas sobre protección de datos por «una autoridad independiente».

El tercer elemento consiste en los compromisos internacionales; el cumplimiento de obligaciones derivadas de instrumentos jurídicamente vinculantes, tales como tratados u otros acuerdos; así como la participación en sistemas o foros multilaterales o regionales, en particular, en materia de protección de datos.

Es así que el artículo 45.2.c) del RGPD indica que se evaluarán

> 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.

V.3. Directrices del Comité Europeo de Protección de Datos

En relación con la evaluación de adecuación del nivel de protección ofrecido por un tercer país, el Comité Europeo de Protección de Datos (CEPD) publicó el documento relativo a las referencias sobre adecuación[5]. Este documento, considerando tanto el RGPD como la jurisprudencia del TJUE, actualiza las directrices en la materia que veinte años antes había adoptado el Grupo de Trabajo del Artículo 29 (1988).

La finalidad de este documento (Comité Europeo de Protección de Datos, 2018c, p. 1) es ofrecer orientación a la Comisión Europea —en virtud del RGPD— y, a su vez, a los terceros países que se plantean obtener la adecuación en torno a la evaluación del nivel de protección de los datos en terceros países. En particular, expone los principios básicos sobre protección de datos que deben estar presentes en el marco jurídico de un tercer país con la finalidad de garantizar una equivalencia esencial con el marco de la Unión Europea.

Atendiendo específicamente a los principios generales en materia de protección de datos para garantizar que el nivel de protección de un tercer país es sustancialmente equivalente al garantizado por la legislación de la Unión Europea, los elementos indicados son los que se incluyen a continuación —y que se refieren tanto a los principios relativos al contenido como a los mecanismos sobre el procedimiento y la ejecución—. Los principios relativos al contenido son:

1. La existencia de conceptos o principios básicos sobre protección de datos. Para ello, resulta relevante que reflejen los conceptos previstos en la legislación europea en materia de protección de datos y sean coherentes con estos.
2. Fundamentos del tratamiento lícito y leal para fines legítimos. Ello implica tanto que el tratamiento de datos sea lícito, leal y legítimo; como que existan varias bases de legitimación del tratamiento, tales como el consentimiento, la ejecución de un contrato, el cumplimiento de una obligación legal o el interés legítimo del responsable del tratamiento o de un tercero, siempre que no prevalezcan sobre los intereses del interesado.
3. Principio de limitación de la finalidad. Deberá ser específico y sin perjuicio de que los datos personales puedan tratarse posteriormente para fines que no sean incompatibles con el fin inicial.

5 Adoptado como propio, ya que inicialmente fue publicado por el Grupo de Trabajo del artículo 29 (2018).

4. Principio de calidad de los datos y proporcionalidad. Según este punto, los datos deben ser precisos y, si fuera necesario, actualizados y, por otra parte, adecuados, pertinentes y no excesivos, atendiendo a la finalidad del tratamiento.
5. Principio de retención o conservación de datos. Deberá ser limitado a la necesidad de los fines para los que se tratan.
6. Principio de seguridad y confidencialidad. Implica que tenga que garantizarse la seguridad de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales. A tal fin deberán adoptarse y aplicarse medidas técnicas y organizativas adecuadas, atendiendo al riesgo existente y teniendo en cuenta el estado de la técnica y los costos.
7. Principio de transparencia. Consiste en proporcionar información al interesado sobre el tratamiento de sus datos personales, salvo excepciones, tales como salvaguardar investigaciones penales, la seguridad nacional o el desarrollo de procedimientos judiciales.
8. Derechos de acceso, rectificación, supresión y oposición. El interesado debe poder ejercer fácilmente estos derechos y sin perjuicio de que pueden estar sujetos a límites.
9. Restricciones a transferencias ulteriores que, como indica el CEPD, solo se permitirán cuando otro destinatario (el destinatario de la transferencia ulterior) también esté sujeto a normas (incluidas normas contractuales) que otorguen un nivel de protección adecuado y que tienen por objeto que la transferencia posterior no menoscabe el nivel de protección.

Además, el CEPD ofrece también algunos ejemplos sobre la aplicación de los principios de contenido a algunos tratamientos específicos de datos personales, tales como la mercadotecnia directa o las decisiones automatizadas y la elaboración de perfiles.

Y, por lo que se refiere a los mecanismos relativos al procedimiento y ejecución, son los relativos a:

1. Autoridades de control competentes independientes, lo que implica que deba existir una o varias autoridades de protección de datos y que actúen con completa independencia e imparcialidad.
2. El sistema de protección de datos debe garantizar un buen nivel de cumplimiento; para ello, resulta relevante la existencia de sanciones efectivas y disuasorias con el fin de asegurar el respeto a las normas sobre protección de datos, así como la existencia de sistemas de verificación directa del cumplimiento.

3. Responsabilidad proactiva, lo que significa que el encargado del tratamiento o quienes tratan datos en su nombre cumplan con la normativa aplicable sobre protección de datos.
4. El sistema de protección de datos debe ofrecer apoyo y ayuda a los interesados individuales en el ejercicio de sus derechos y mecanismos de reclamación adecuados.

El CEPD se refiere también, en sus Directrices, a las garantías esenciales en terceros países para el acceso a los datos por parte de los cuerpos policiales y de seguridad a fin de limitar las injerencias en los derechos fundamentales. En concreto, las cuatro garantías (Comité Europeo de Protección de Datos, 2018c, p. 9) que deben respetar los terceros países en lo que se refiere al acceso a los datos, tanto para fines de seguridad nacional como para fines de cumplimiento de la ley, son las siguientes:

1. El tratamiento debe basarse en normas claras, precisas y accesibles (base jurídica).
2. Se debe demostrar la necesidad y la proporcionalidad respecto a los objetivos legítimos perseguidos.
3. El tratamiento debe estar sujeto a una supervisión independiente.
4. Las personas deben disponer de vías de acción efectivas.

En definitiva, el CEPD, a partir de la legislación y la jurisprudencia europea en materia de protección de datos, trata de ofrecer directrices sobre el contenido o derecho sustantivo y procedimental o derecho procesal a considerar en la evaluación de la adecuación del nivel de protección ofrecido por un tercer país.

V.4. La aplicación extraterritorial del RGPD

Una cuestión relevante que considerar es la relativa a la aplicación extraterritorial del RGPD. En concreto, el artículo 3 del RGPD incluye dos situaciones en las que este es aplicable más allá de las fronteras de la Unión Europea. Se trata de los casos en los que un responsable o encargado del tratamiento que no está establecido en la Unión Europea:

1. Trata datos personales relativos a la oferta de bienes o servicios a interesados que se encuentran en la Unión Europea, con independencia de que se les requiera un pago.
2. O controla el comportamiento de interesados que se encuentran en la Unión Europea.

Es decir, se requiere una doble condición para que el RGPD sea aplicable en este caso. Por una parte, es necesario que se traten datos de interesados que se encuentren en la Unión Europea, ya sea por la oferta

de bienes o servicios o por el control del comportamiento. Por otra parte, resulta imprescindible que se dirijan a interesados que se encuentren en dicho territorio.

Por lo que se refiere, en particular, a determinar si un responsable o encargado del tratamiento ofrece bienes o servicios a interesados que se encuentran en la Unión Europea, el considerando 23 del RGPD explica que debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Y, al respecto, continúa explicando también que

> [s]i bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

En relación con lo anterior, el Comité Europeo de Protección de Datos publicó, a finales de 2018, un borrador de directrices sobre el artículo 3 del RGPD, para consulta pública, en el que analiza el criterio de focalización (en inglés, *targeting criterion*) (2018b). Estas directrices tratan de dar respuesta a dudas y cuestiones que se plantean en relación con el citado artículo. Es decir, se trata de garantizar el cumplimiento del RGPD, si bien en determinadas situaciones se requiere un análisis caso por caso para determinar si el RGPD es aplicable al tratamiento de datos personales por un responsable o encargado del tratamiento.

Sin perjuicio de lo anterior, cabe considerar también el caso de los encargados del tratamiento que están fuera del Espacio Económico Europeo y traten datos personales por cuenta del responsable del tratamiento o, a su vez, de otro encargado del tratamiento establecidos en dicho territorio. Estos encargados del tratamiento tienen que ofrecer garantías suficientes para cumplir con el RGPD. En concreto, el artículo 28 del RGPD obliga al responsable del tratamiento a elegir únicamente a un encargado del tratamiento que ofrezca garantías suficientes para cumplir con el RGPD, con independencia de dónde se encuentre establecido este.

VI. ¿QUÉ ES UNA DECISIÓN DE ADECUACIÓN DE LA COMISIÓN EUROPEA?

Una decisión de adecuación de la Comisión Europea es un acto jurídico del derecho de la Unión Europea (Borchardt, 2017, p. 111) en virtud del cual se facilita, como garantía adecuada, la libre circulación de datos personales a terceros países desde la UE, sin que sean necesarias garantías adicionales o cumplir otras condiciones (Comisión Europea, 2017, p. 4). En concreto, en materia de nivel adecuado en protección de datos, una decisión de la Comisión Europea es una decisión unilateral de ejecución, adoptada en virtud de la legislación sobre protección de datos personales y conforme a los criterios fijados en esta. El efecto de la decisión es constatar que un país tercero ofrece un nivel de protección de datos personales sustancialmente equivalente al que se garantiza en la Unión Europea, lo que implica considerar tanto la Carta de los Derechos Fundamentales de la Unión Europea como la legislación sobre protección de datos.

Desde la entrada en vigor de la directiva 95/46/CE, los terceros países que han obtenido una decisión de nivel adecuado son (en orden alfabético): 1) Andorra, 2) Argentina, 3) Canadá, 4) Estados Unidos de América (Escudo de Privacidad), 5) Guernsey, 6) Isla de Man, 7) Islas Feroe, 8) Israel, 9) Japón, 10) Jersey, 11) Nueva Zelanda, 12) Suiza, y 13) Uruguay.

Como referencia histórica, la Comisión Europea emitió otras dos decisiones de adecuación en la misma fecha. La primera de ellas, la decisión 2000/519/CE de la Comisión, del 26 de julio de 2000, fue formulada con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Hungría. El hecho de que Hungría accediese, en 2004, a la Unión Europea dejó sin efecto la citada decisión de adecuación.

Y, en segundo lugar, se emitió la decisión 2000/520/CE de la Comisión, del 26 de julio de 2000, con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo. En este caso, la decisión se ocupaba de la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Esta decisión fue la primera en la materia, y por el momento única, anulada por el Tribunal de Justicia de la Unión Europea.

Ahora bien, se trata de apenas trece países en dos décadas de aplicación de la normativa europea sobre protección de datos —primero la ya derogada directiva 95/46/CE y ahora el RGPD—. Además, en relación con el listado de países que han obtenido hasta el momento una decisión de adecuación, la Comisión Europea ha explicado en la

comunicación ya citada que son países que: 1) tienen lazos estrechos con la Unión Europea y sus Estados miembros (Suiza, Andorra, las Islas Feroe, Guernesey, Jersey y la Isla de Man); 2) son importantes socios comerciales (Argentina, Canadá, Israel, los Estados Unidos y Japón), o 3) son países pioneros en la elaboración de leyes en su región (Nueva Zelanda y Uruguay). Es decir, se trata de un limitado número de países, lo que debe hacer reflexionar sobre si el modelo de nivel adecuado así planteado es la aproximación apropiada para lograr objetivos como los ya indicados.

VII. LA DECISIÓN DE ADECUACIÓN DE JAPÓN

La decisión de ejecución (UE) 2019/419 de la Comisión —del 23 de enero de 2019, sobre el nivel adecuado en protección de datos proporcionado por Japón— es la primera que se adoptó y publicó después del 25 de mayo de 2018, fecha a partir de la que se aplica de manera efectiva el RGPD. Además, es también la primera decisión de adecuación que se refiere a una transferencia mutua de datos personales entre la Unión Europea y Japón.

La decisión se divide en ciento noventa considerandos, cuatro artículos y dos anexos, refiriéndose estos últimos, respectivamente, a las reglas complementarias adoptadas por la Comisión de Protección de la Información Personal (CPIP) y a las declaraciones, garantías y compromisos oficiales asumidos por el Gobierno japonés frente a la Comisión Europea. Es relevante que en los considerandos se explica el contenido de la decisión a partir de los elementos previstos en el artículo 45 del RGPD y considerando también las directrices del CEPD —en particular, en lo que se refiere tanto al contenido del marco de protección de datos en Japón como a las garantías esenciales en el caso del acceso a los datos por parte de los cuerpos policiales y de seguridad a fin de limitar las injerencias en los derechos fundamentales—.

Es así que, tras una breve introducción, la Comisión Europea dedica un apartado a la normativa aplicable al tratamiento de datos personales. En él, se refiere al marco de protección de datos japonés: así, se ocupa de su ámbito de aplicación material y personal, atendiendo en particular a los conceptos o definiciones; de las salvaguardas, derechos y obligaciones que se refieren tanto a los principios de protección de datos como a los derechos de los interesados y a las obligaciones de quienes tratan datos personales; de la supervisión y control de la aplicación de la normativa por una autoridad de protección de datos independiente —que, en el caso de Japón, es la CPIP—; del acceso a recursos judiciales, así como de las garantías esenciales referidas al acceso y la utilización por las autoridades públicas japonesas de datos personales transferidos desde la

Unión Europea, tanto a efectos de control de la aplicación del derecho penal como a efectos de seguridad nacional.

A continuación, los considerandos hacen referencia a la conclusión sobre el nivel de protección adecuado proporcionado por Japón para la transferencia de datos desde la Unión Europea. También los considerandos se refieren a la actuación de las autoridades de protección de datos en la Unión Europea, en cuanto a que pudieran recibir consultas o reclamaciones, de las que los Estados miembros deberán informar a la Comisión Europea. Asimismo, se menciona que la información sobre cualquier novedad relevante para la decisión de adecuación debe ser proporcionada por las autoridades japonesas. Finalmente, se hace referencia a la supervisión continua por parte de la Comisión Europea de que Japón proporciona el nivel adecuado.

Por lo que se refiere a la revisión de la decisión, otro de los apartados, que incluye varios considerandos, prevé que, conforme al RGPD, se revise periódicamente si las constataciones relativas a la adecuación del nivel de protección garantizado por Japón siguen estando justificadas desde el punto de vista factual y legal (considerando 180). Y también se explica, en otro apartado, la potestad de la Comisión Europea de suspender la decisión de adecuación si concluyera que el nivel adecuado de protección no pudiera considerarse equivalente en lo esencial al de la Unión Europea.

Por último, cabe señalar que las decisiones de adecuación que fueron publicadas antes del 25 de mayo de 2018 tienen que ser revisadas conforme a los requisitos del RGPD. Al respecto, la Comisión Europea indicó, en su comunicación 374 final (Comisión Europea, 2019), que en 2020 proporcionará información sobre la revisión de las decisiones de adecuación que fueron adoptadas conforme a la directiva 95/46/CE

VIII. ENFOQUE EN AMÉRICA LATINA

VIII.1. Legislación nacional

Por lo que se refiere al enfoque de América Latina en cuanto al nivel de protección adecuado proporcionado por terceros países para la transferencia internacional de datos, podemos considerar, por una parte, a los países que ya cuentan con el nivel adecuado de la Unión Europea —es decir, Argentina y Uruguay—.Por otra parte, debemos tomar también en cuenta a los países que cuentan con legislación sobre protección de datos desde hace años o recientemente, como son los casos de Brasil, Colombia, México y Perú. En particular, atenderemos a continuación a estos últimos.

VIII.1.1. Brasil

Tras varios años y propuestas, Brasil publicó la Ley 13.709 de protección de datos personales. Entre las definiciones incluidas en el artículo 5, se encuentra, en la fracción XV, la de «transferencia internacional de datos». Esta noción es definida como la transferencia de los datos personales a un país extranjero u organismo internacional del que el país sea miembro. La ley dedica su capítulo V, artículos 33 a 36, a la transferencia internacional de datos.

Al respecto, el artículo 33 requiere que, para poder llevar a cabo una transferencia internacional de datos, esta tenga lugar cuando se dé alguno de los supuestos previstos, entre los que se encuentran los siguientes: que los países u organismos internacionales proporcionen un nivel adecuado conforme al previsto en la ley; o que el responsable del tratamiento proporcione y compruebe que existen garantías de cumplimiento de los principios, de los derechos de los interesados y del régimen de protección de datos previsto en la Ley Brasileña —en la forma, por ejemplo, de normas corporativas globales—. Es decir, Brasil incluye en su ley sobre protección de datos tanto el enfoque del nivel adecuado, tratándose en este caso de un estándar nacional, como las garantías adecuadas proporcionadas por el responsable del tratamiento.

VIII.1.2. Colombia

En el caso de Colombia, la Ley 1581 por la cual se dictan disposiciones generales para la protección de datos personales regula las transferencias internacionales de datos en su título VIII, artículo 26. En concreto, en el citado artículo, la ley establece la regla general, que consiste en de prohibir la transferencia internacional de datos «a países que no proporcionen un nivel adecuado de protección de datos». Y define el nivel adecuado de protección de datos del siguiente modo:

> un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios (artículo 26).

Al respecto, la Superintendencia de Industria y Comercio, de la que depende la Delegatura de Protección de Datos[6], publicó en 2018 una Circular Única en cuyo capítulo tercero se incluyen los estándares del nivel adecuado de protección de datos del país receptor, la lista de países con nivel adecuado y la declaración de conformidad.

Por lo que se refiere a los estándares aplicables para determinar si el país receptor de la información personal, se mencionan los siguientes criterios:

6 Véase al respecto el sitio web de la Superintendencia (http://www.sic.gov.co/).

1. Existencia de normas aplicables al tratamiento de datos personales.
2. Consagración normativa de principios aplicables al tratamiento de datos; entre otros: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
3. Consagración normativa de derechos de los titulares.
4. Consagración normativa de deberes de los responsables y encargados.
5. Existencia de medios y vías judiciales y administrativas para garantizar la tutela efectiva de los derechos de los titulares y exigir el cumplimiento de la ley.
6. Existencia de autoridad(es) pública(s) encargada(s) de la supervisión del tratamiento de datos personales, del cumplimiento de la legislación aplicable y de la protección de los derechos de los titulares, que ejerza(n) de manera efectiva sus funciones.

En cuanto a la lista de países con nivel adecuado, se incluyen los veintiocho países miembros de la Unión Europea; dos de los tres países del EEE, pero no Liechtenstein, pese a que cumple con los mismos requisitos que aquellos; Serbia, Costa Rica, México, Perú, Australia, Japón, Estados Unidos de América, República de Corea, así como los países que han sido declarados con el nivel adecuado de protección por la Comisión Europea. Se debe tener en cuenta que algunos de estos países son mencionados por separado en la Circular Única. Y, al respecto, la lista podrá ser objeto de revisión para incluir a otros países o excluir a otros de la lista.

VIII.1.3. México

El caso de México, con referencia específicamente al sector privado, donde aplica la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, señala con respecto a quienes participan que puede haber tanto una transferencia de datos entre dos responsables del tratamiento como una remisión entre un responsable y un encargado del tratamiento. Ambas pueden ser internacionales.

En concreto, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares prevé la posibilidad de llevar a cabo transferencias internacionales de datos cuando concurran garantías adecuadas. En este sentido, el artículo 74 indica que «las transferencias internacionales de datos personales serán posibles cuando el receptor de los datos personales asuma las mismas obligaciones que corresponden al responsable que transfirió los datos personales».

Ahora bien, el artículo 37 de la ley, salvo las excepciones previstas en el mismo, requiere como norma general el consentimiento del interesado. Al respecto, en el Reglamento de la ley, por lo que se refiere a la formalización de la transferencia internacional, prevé que en las cláusulas contractuales u otros instrumentos, como podrían ser las normas corporativas vinculantes, se incluyan «las condiciones en las que el titular consintió el tratamiento de sus datos personales».

Por otra parte, en el artículo 52 del Reglamento, relativo al tratamiento de datos personales en el denominado cómputo en la nube, se incluyen los requisitos exigibles a los proveedores de estos servicios, con independencia de dónde se encuentren. En cualquier caso, se debe prestar atención al hecho de que lo que se requiere son garantías adecuadas tanto por parte del responsable del tratamiento como del proveedor de los servicios. En efecto, en términos de prohibición o limitación, el citado artículo prevé expresamente que el responsable del tratamiento no pueda adherirse a servicios que no garanticen la debida protección de los datos personales. Por lo tanto, México es de los países de América Latina que más se acercan a la aproximación basada en garantías proporcionadas por el responsable del tratamiento.

VIII.1.4. Perú

En Perú, la Ley 29733 de protección de datos personales define el flujo transfronterizo de datos como «la transferencia a un destinatario situado en otro país, con independencia de cuál sea el soporte en el que se encuentren, los medios por los cuáles se efectúe o el tratamiento que reciban los datos personales» (artículo 2, apartado 8). Y define también qué es el nivel suficiente de protección para los datos personales, indicando, en el apartado 10 del artículo 2, que es «el nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate».

En concreto, en el artículo 15, relativo al flujo transfronterizo de datos, la ley sujeta este a la exigencia de que el país destinatario proporcione niveles de protección adecuados. Además, prevé que si el país destinatario no tiene un nivel adecuado, «el emisor del flujo transfronterizo tenga que garantizar que el tratamiento de los datos personales se efectúe conforme a lo previsto en» la ley, sin perjuicio de que, a continuación, se prevean un listado de excepciones a lo anterior. Es decir, si el país destinatario no proporciona un nivel de protección adecuado, el flujo transfronterizo de los datos será posible si concurre alguna de las situaciones previstas, tales como la necesidad de los datos personales para la ejecución de una relación contractual en la que el interesado es parte; el que se trate de una transferencia bancaria; o cuando el interesado haya dado su consentimiento previo, informado, expreso e inequívoco.

VIII.2. Estándares de Protección de Datos Personales

Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos fueron adoptados, por unanimidad, el 20 de junio de 2017, en el marco del XV Encuentro Iberoamericano de Protección de Datos de la Red Iberoamericana de Protección de Datos (RIPD). En concreto, el capítulo V de los Estándares está dedicado a las transferencias internacionales de datos. Si bien hubiera sido deseable una expresa indicación de la libre transferencia internacional de datos, cuando se den las garantías adecuadas, el numeral 36, relativo a las reglas generales, lista en su apartado 1 los mecanismos a los que podrá recurrirse para llevar a cabo la transferencia internacional de datos. Al respecto, cabe destacar que la letra a) es la relativa al mecanismo de adecuación, si bien, a diferencia del enfoque europeo, se prevé que el país destinatario o varios sectores del mismo puedan acreditar las condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado. No obstante, a pesar de que existe esta posibilidad, en última instancia ella va a depender del reconocimiento del país de origen de la transferencia, a menos que se prevea algún procedimiento al efecto, lo cual sería deseable.

Por lo que se refiere al mecanismo de garantías suficientes proporcionadas por el responsable, la letra b) del apartado 1 del numeral 36 indica que el exportador de los datos puede ofrecer garantías suficientes «del tratamiento de los datos personales en el país destinatario». Asimismo, indica que es necesario que este último «acredite el cumplimiento de las condiciones mínimas y suficientes establecidas en la legislación nacional de cada Estado Iberoamericano aplicable en la materia».

Por último, el apartado 2 del citado numeral incluye los supuestos en los que la legislación nacional puede establecer expresamente límites a las transferencias internacionales de datos, entendiendo que se trata de una lista cerrada o *numerus clausus* por la redacción dada. Esta lista incluye los supuestos relativos a la seguridad nacional, la seguridad pública, la protección de la salud pública, la protección de los derechos y libertades de terceros, así como aquellos vinculados a cuestiones de interés público.

IX. OTROS PAÍSES

Una cuestión que puede plantearse es que existen países que no tienen nivel adecuado de protección de datos otorgado por la Comisión Europea ni por otros países, pero que, sin embargo, sí son parte del Consejo de Europa y han por tanto firmado y ratificado el Convenio 108 —actualmente debe tenerse en cuenta que tendrá que tratarse de su versión actualizada—. Asimismo, también existen países que, aún no siendo parte del Consejo, accedieron al Convenio. Por ejemplo, además de Uruguay, son terceros países miembros del Consejo de

Europa Albania y Turquía; a su vez, no son parte del Consejo de Europa, pero han accedido al Convenio 108, países como Mauricio o México.

En este sentido, es necesario tener en cuenta que el ya mencionado artículo 12 del Convenio 108 indicaba en su apartado 2 que una parte no puede prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra parte. Es así que cabría preguntarse si la consideración de Turquía como tercer país sin nivel adecuado no acaba convirtiéndose en una prohibición de libre flujo de los datos personales.

En otras palabras, cabe plantearse al respecto por qué en estos casos se exige proporcionar garantías adecuadas, cuando los países ya son parte del Convenio 108. Si no las hubiera, se exige autorización previa de la autoridad de protección de datos desde el país exportador en la Unión Europea. Parece que, pese a los avances en la normativa europea sobre protección de datos en la Unión Europea, queda claro que, si hay una decisión de adecuación de la Comisión Europea, ya no es necesaria una autorización de la autoridad de protección de datos. Sin embargo, todavía se plantean casos en los que no debería ser exigible garantía adicional alguna por el hecho de ser parte de un instrumento jurídico internacional vinculante en materia de protección de datos. Es decir, por ejemplo, una transferencia internacional de datos desde España a México no debería requerir nada más, ya que se trata de un tercer país que es parte del Convenio 108.

X. ¿POR QUÉ DEBERÍA CONSIDERARSE UN ESTÁNDAR MULTILATERAL PARA FACILITAR LAS TRANSFERENCIAS INTERNACIONALES DE DATOS?

Actualmente, un enfoque unilateral con respecto al nivel adecuado de protección para las transferencias internacionales de datos ni es suficiente ni es adecuado. Los instrumentos internacionales en materia de protección de datos, ya mencionados, se publicaron en el siglo pasado. Como es evidente, desde entonces se ha producido un importante avance, en muchos sentidos, que ha dado paso al momento actual. Al respecto, sería conveniente encontrar un punto de equilibrio que, aplicado al concepto de nivel adecuado, dé lugar a establecer los parámetros que sirvan de guía para dar un próximo paso en el fortalecimiento de la protección de las personas respecto del tratamiento de los datos personales (Maqueo, Moreno & Recio, 2017, p. 79).

Un estándar —como el nivel adecuado de protección de datos para la transferencia internacional de datos— adoptado unilateralmente plantea grandes retos en la práctica. Mientras que un país o una región cuenta con un listado de países, otro país puede, por un lado, tener un

listado distinto e, incluso, por otro lado, no tener el nivel adecuado para otros países o regiones. El complejo escenario al que da lugar esta situación, ya que resulta muy difícil poder encontrar caminos libres de obstáculos, no es el adecuado.

El libre flujo internacional de los datos personales tiene que ser también resguardado frente a medidas proteccionistas que, en última instancia, dan lugar a barreras comerciales o afectan gravemente a otros derechos —tales como el derecho a la libertad de expresión o al acceso a la información—, al impedir el ejercicio de estos. Incluso, pueden tener otras consecuencias negativas relevantes, como obstaculizar la generación de trabajo —al impedir que, por ejemplo, un emprendedor pueda prestar servicios fuera del país en el que está establecido al encontrar obstáculos si una empresa de otro país quiere recurrir a él—.

Y este libre flujo será más fácil y, sobre todo, apropiado de alcanzar, si, en el caso del mecanismo del nivel de protección adecuado para la transferencia internacional de datos, se considera un enfoque multilateral. Esto permitirá, entre otras cuestiones, responder mejor a los retos existentes o que se pueda plantear y garantizar una protección realmente efectiva. Además, el enfoque multilateral podría ayudar también a lograr la estabilidad necesaria, evitando así turbulencias que pueden dar lugar a incertidumbres jurídicas —como ocurrió en el caso de la anulación del Acuerdo de Puerto Seguro entre la Unión Europea y los Estados Unidos—.

En definitiva, existen diversos motivos relevantes, tales como los apuntados, para preferir un enfoque multilateral a la hora de seguir desarrollando el nivel de protección adecuado como instrumento para la transferencia internacional de datos. Además, el nivel adecuado no es la única opción, ya que existen otros instrumentos como, por ejemplo, recurrir a garantías adecuadas basadas en instrumentos jurídicamente vinculantes entre el exportador y el importador de los datos. Estos instrumentos alternativos son también relevantes y plantean la importancia de considerar las ventajas y desventajas en cada caso.

XI. CONCLUSIONES

En virtud de las cuestiones analizadas en los apartados anteriores, cabe presentar las conclusiones que se exponen a continuación. En primer lugar, el nivel adecuado en protección de datos para las transferencias internacionales de datos fue incluido por primera vez en las Directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE) y el Convenio 108 del Consejo de Europa. Estos instrumentos no definieron este concepto. En el caso de la Unión Europea, en particular el Reglamento General de Protección de Datos (RGPD) ha

incluido los elementos específicos que deben ser considerados a la hora de evaluar el nivel de protección ofrecido por un tercer país para decidir si se le otorga o no el nivel adecuado para transferencias internacionales de datos.

En segundo lugar, el concepto de nivel adecuado, aunque no ha sido definido ni en la directiva 95/46/CE ni en el RGPD, ha tenido un desarrollo más amplio durante las últimas décadas en la Unión Europea. En este sentido, el reconocimiento del nivel adecuado, a efectos de la Unión Europea, se ha otorgado por la Comisión Europea a trece países hasta la fecha. Se trata de un número reducido de países si consideramos que, aproximadamente, 132 países alrededor del mundo cuentan con leyes sobre protección de datos o privacidad y, de estos, treinta y uno son países de la Unión Europea y del Espacio Económico Europeo. Es decir, los países que para la Unión Europea tienen un nivel adecuado siguen siendo un pequeño porcentaje a fecha de hoy.

En tercer lugar, el RGPD ha supuesto una evolución con respecto a las transferencias internacionales de datos y también a los elementos que deben considerarse en cuanto al nivel de protección adecuado. Estos elementos son el Estado de Derecho —lo que incluye la legislación, la jurisprudencia, los derechos efectivos y exigibles, y el acceso a la justicia por los interesados cuyos datos personales sean objeto de transferencia a un tercer país—; la existencia y el funcionamiento efectivo de una o varias autoridades de protección de datos o autoridades de control independientes; y, por último, los compromisos internacionales; el cumplimiento de obligaciones derivadas de instrumentos jurídicamente vinculantes, tales como tratados u otros acuerdos; así como la participación en sistemas o foros multilaterales o regionales en la materia.

Un claro ejemplo de la aplicación de estos elementos se encuentra en la decisión de adecuación de Japón. Se trata de la primera decisión de adecuación otorgada por la Comisión Europea después del 25 de mayo de 2018, fecha de aplicación efectiva del RGPD. Además, es también la primera que hace referencia a la transferencia mutua de datos personales. En cuanto a las demás decisiones de adecuación, están siendo objeto de revisión y la Comisión Europea informará al respecto durante el año 2020.

En cuarto lugar, algunos países de América Latina han incluido también en sus legislaciones el concepto de nivel adecuado de protección de datos para la transferencia internacional de datos —como Brasil, Colombia y Perú—. En concreto, estos países han incluido el concepto de nivel adecuado en sus leyes sobre protección de datos. Y también se ha seguido este criterio en los Estándares de Protección de Datos Personales, aprobados por Red Iberoamericana de Protección de Datos (RIPD).

En quinto lugar, el modelo de adecuación, que se basa en el nivel adecuado del país al que se van a exportar los datos personales, es una de las opciones posibles, Sin embargo, no es la única, ya que existen otras —como ofrecer garantías suficientes por las partes de la transferencia internacional de datos, ya sean responsables o encargados del tratamiento—.

Por último, cabría plantear si el nivel adecuado, como mecanismo respecto de las transferencias internacionales de datos, requeriría de una aproximación multilateral. Una definición unilateral o parcial puede no ser adecuada —ya que puede producirse una situación de falta de reciprocidad; es decir, mientras que un país incluye en su lista de terceros países con nivel adecuado de protección de datos para transferencias internacionales a otro país o región, puede que estos últimos no hagan lo propio con el primero—. Por lo tanto, una aproximación multilateral podría ser más correcta, sin perjuicio de que, en cualquier caso, el modelo de adecuación no es la única opción para las transferencias internacionales de datos, ya que existen otros mecanismos que deben ser considerados.

REFERENCIAS

Borchardt, K. (2017). *El ABC del Derecho de la Unión Europea, Comisión Europea*. Luxemburgo: Oficina de Publicaciones de la Unión Europea. Recuperado de http://publications.europa.eu/resource/cellar/5d4f8cde-de25-11e7-a506-01aa75ed71a1.0021.01/DOC_1

Comisión Europea (2017). *Comunicación de la Comisión al Parlamento Europeo y al Consejo: intercambio y protección de datos personales en un mundo globalizado*. COM(2017) 7 final. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007&qid=1559205331387&from=ES.

Comisión Europea (2019). *Communication from the Commission to the European Parliament and the Council: data protection rules as a trust-enabler in the EU and beyond –taking stock*. COM(2019) 374 final. Recuperado de https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0374&qid=1567072717840&from=ES

Comité Europeo de Protección de Datos (CEPD) (2018a). *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*. 25 de mayo. Recuperado de https://edpb.europa.eu/our-work-tools/our-documents/nasoki/guidelines-22018-derogations-article-49-under-regulation-2016679_en

Comité Europeo de Protección de Datos (CEPD) (2018b). *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation*. 16 de noviembre. Recuperado de https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf

Comité Europeo de Protección de Datos (CEPD) (2018c). *Referencias sobre adecuación*, aprobado el 28 de noviembre de 2017, revisado por última vez y aprobado el 6 de febrero de 2018. Recuperado de https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=54200

Consejo de Europa (2018). *The modernised Convention 108: novelties in a nutshell*. Recuperado de https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8.

Greenleaf, G. (2019). Global Tables of Data Privacy Laws and Bills (6ª ed.). Supplement to 157 *Privacy Laws & Business International Report* (PLBIR). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3380794

Grupo de Trabajo del artículo 29 (1998). *Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. DG XV D/5025/98, WP 12*. Aprobado el 24 de julio de 1998. Recuperado de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_es.pdf

Grupo de Trabajo del Artículo 29 (2018). *Referencias sobre adecuación, WP 254 rev. 01*. Aprobado el 28 de noviembre de 2017, revisado por última vez y aprobado el 6 de febrero de 2018. Recuperado de https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=54200

GSMA (2018). *Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation*. Recuperado de https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf

Kuner, C. (2017). Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, *18*(881). Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346

Maqueo Ramírez, M.S., Moreno González, J., & Recio Gayo, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho*, *XXX*(1), 77-96. Recuperado de https://scielo.conicyt.cl/pdf/revider/v30n1/art04.pdf

Organisation for Economic Co-Operation and Development (OECD) (2013). *The OCDE Privacy Framework*. Recuperado de http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf#_ga=2.20480760.1147834656.1559116688-1378050382.1557067453

Organisation for Economic Co-Operation and Development (OECD) (2018). *Working Party of the Trade Committee. Trade and Cross-Border Data Flows*. Recuperado de http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)19/FINAL&docLanguage=En

Parlamento Europeo (2016). *Directorate-General for External Policies, Policy Departament. Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's and External Policies*. Recuperado de http://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU%282016%29535006_EN.pdf

United Nations Conference on Trade and Development (UNCTAD). (2016). *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Nueva York-Ginebra: Naciones Unidas. Recuperado de https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

Jurisprudencia, normativa y otros documentos legales

Acuerdo General sobre el Comercio de Servicios de la Organización Mundial del Comercio (OMC). Entrada en vigor en enero de 1995.

Carta de los Derechos Fundamentales de la Unión Europea.

Circular Única. Circular del 28 de marzo de 2018 de la Superintendencia de Industria y Comercio.

Convenio 108. Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Estrasburgo, 28 de enero de 1981.

Decisión 2000/518/CE. Decisión de la Comisión, del 26 de julio de 2000, con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza [notificada con el número C(2000) 2304] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 215 (25 de agosto de 2000). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1557085318222&uri=CELEX:32000D0518

Decisión 2000/519/CE. Decisión de la Comisión, del 26 de julio de 2000, con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Hungría [notificada con el número C(2000) 2305] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L., num. 215. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32000D0519

Decisión 2000/520/CE. Decisión de la Comisión, del 26 de julio de 2000, con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América [notificada con el número C(2000) 2441] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, num. 215. Recuperado de https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32000D0520

Decisión 2001/497/CE. Decisión de la Comisión, Decisión de la Comisión, del 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la directiva 95/46/CE [notificada con el número C(2001) 1539] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, num. 181 (04 de julio de 2001). Recuperado de https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32001D0497

Decisión 2002/2/CE. Decisión de la Comisión, del 20 de diciembre de 2001, con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley

canadiense Personal Information and Electronic Documents Act [notificada con el número C(2001) 4539]. *Diario Oficial de la Unión Europea*, serie L, núm. 2 (4 de enero de 2002). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1557085577618&uri=CELEX:32002D0002

Decisión 2003/490/CE. Decisión de la Comisión, del 30 de junio de 2003, con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 168 (5 de julio de 2003). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1557084451785&uri=CELEX:32003D0490

Decisión 2003/821/CE. Decisión de la Comisión, del 21 de noviembre de 2003, relativa al carácter adecuado de la protección de los datos personales en Guernsey [notificada con el número C(2003) 4309] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 308 (25 de noviembre de 2003). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1557084510929&uri=CELEX:32003D0821

Decisión 2004/411/CE. Decisión de la Comisión, del 28 de abril de 2004, relativa al carácter adecuado de la protección de los datos personales en la Isla de Man [notificada con el número C(2004) 1556] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 151 (30 de abril de 2004). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32004D0411&qid=1557084670440&from=ES

Decisión 2004/915/CE. Decisión de la Comisión, del 27 de diciembre de 2004, por la que se modifica la decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países [notificada con el número C(2004) 5271] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, num. 385. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32004D0915

Decisión 2008/393/CE. Decisión de la Comisión, del 8 de mayo de 2008, de conformidad con la directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Jersey [notificada con el número C(2008) 1746] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 138 (28 de mayo de 2008). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1557085136487&uri=CELEX:32008D0393.

Decisión 2010/146/UE. Decisión de la Comisión, del 5 de marzo de 2010, con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada dada en la Ley de las Islas Feroe sobre el tratamiento de datos personales [notificada con el número C(2010) 1130] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 58 (9 de marzo de 2010). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1557084777039&uri=CELEX:32010D0146

Decisión 2010/625/UE. Decisión de la Comisión, del 19 de octubre de 2010, de conformidad con la directiva 95/46/CE del Parlamento Europeo y del Consejo,

relativa a la adecuada protección de los datos personales en Andorra [notificada con el número C(2010) 7084] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 277 (21 de octubre de 2010). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1557084236172&uri=CELEX:32010D0625

Decisión 2010/87/CE. Decisión de la Comisión, del 5 de febrero de 2010 , relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la directiva 95/46/CE del Parlamento Europeo y del Consejo [notificada con el número C(2010) 593] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, num. 39. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32010D0087

Decisión 2011/61/UE. Decisión de la Comisión, del 31 de enero de 2011, de conformidad con la directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por el Estado de Israel en lo que respecta al tratamiento automatizado de los datos personales [notificada con el número C(2011) 332] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 27 (1 de febrero de 2011). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1557084842312&uri=CELEX:32011D0061

Decisión de Ejecución (UE) 2016/1250. Decisión de la Comisión, del 12 de julio de 2016, con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU. [notificada con el número C(2016) 4176] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 207 (1 de agosto de 2016). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1557085722663&uri=CELEX:32016D1250

Decisión de Ejecución (UE) 2019/419. Decisión de la Comisión, de 23 de enero de 2019, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 76 (19 de marzo de 2019). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1557085844413&uri=CELEX:32019D0419

Decisión de Ejecución 2012/484/UE. Decisión de la Comisión, del 21 de agosto de 2012, de conformidad con la directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales [notificada con el número C(2012) 5704] (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 227 (23 de agosto de 2012). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1557085422448&uri=CELEX:32012D0484

Decisión de Ejecución 2013/65/UE. Decisión de la Comisión, del 19 de diciembre de 2012, de conformidad con la directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por Nueva Zelanda [notificada con el número C(2012) 9557] (texto pertinente a efectos del

EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 28 (30 de enero de 2013). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1557085232834&uri=CELEX:32013D0065

Directiva 95/46/CE. Directiva del Parlamento Europeo y del Consejo, del 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. *Diario Oficial de la Unión Europea*, serie L, núm. 281 (23 de noviembre de 1995). Recuperada de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1559204767525&uri=CELEX:31995L0046

Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales. Adoptadas el 23 de setiembre de 1980. Recuperadas de http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part5

Estándares de Protección de Datos Personales para los Estados Iberoamericanos. Adoptados por unanimidad el 20 de junio de 2017, en el marco del XV Encuentro Iberoamericano de Protección de Datos de la Red Iberoamericana de Protección de Datos (RIPD).

Ley 13.709 [Brasil]. Lei geral de proteção de dados pessoais. Congresso Nacional. 14 de agosto de 2018. *Diário Oficial da União*, 15 de agosto de 2018. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Ley 1581 [Colombia]. Ley por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de Colombia. 17 de octubre de 2012. Recuperada de http://www.sic.gov.co/sites/default/files/normatividad/Ley_1581_2012.pdf

Ley 29733 [Perú]. Ley de protección de datos personales. Congreso de la República del Perú. 21 de junio de 2011. *Diario Oficial El Peruano*, 3 de julio de 2011. Recuperado de https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares [México]. Cámara de Diputados. 27 de abril de 2010. *Diario Oficial de la Federación*, 05 de julio de 2010. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Maximillian Schrems c. Data Protection Commissioner. Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) del 6 de octubre de 2015. Asunto C-362/14. ECLI:EU:C:2015:650.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares [México]. Cámara de Diputados. 19 de diciembre de 2011. *Diario Oficial de la Federación*, 21 de diciembre de 2011. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

Reglamento General de Protección de Datos (RGPD). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 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) (texto pertinente a efectos del EEE). *Diario Oficial de la Unión Europea*, serie L, núm. 119 (4 de mayo de 2016). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1559205159718&uri=CELEX:32016R0679

Recibido: 30/05/2019
Aprobado: 10/09/2019