Transferencias internacionales de datos personales

PID_00248556

Cristina Blasi Casagran

Tiempo mínimo de dedicación recomendado: 3 horas

Universitat Oberta de Catalunya

Índice

Introducción..... 5

1. Marco legal aplicable..... 7

2. Transferencias internacionales con países que no aseguren un nivel adecuado de protección..... 11
2.1. Cláusulas contractuales tipo 12
2.2. Normas Corporativas Vinculantes 13
2.3. Códigos de conducta y garantías *ad hoc*..... 15
2.4. Otras excepciones 16

3. Escudo de la Privacidad UE-EEUU..... 18

4. El Acuerdo Marco de protección de datos entre la UE y EEUU..... 25

Resumen..... 29

Bibliografía..... 31

Introducción

El Reglamento general de protección de datos (RGPD) no contiene una definición detallada de lo que se entiende como «transferencia internacional», y tampoco define lo que se entiende por tercer país. Por lo que respecta al concepto de «tercero», se debe entender que son aquellos países que se encuentran fuera del territorio del Espacio Económico Europeo. En cuanto a Gran Bretaña, será necesario precisar cuál va a ser su estatus cuando salga formalmente de la UE, tras el referéndum sobre el Brexit y el inicio del procedimiento de retirada según el artículo 50 TFUE.

Así pues, una **transferencia internacional de datos** se puede definir como un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), 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 de uno de los Estados miembros de la Unión Europea.

Como regla general, para realizar transferencias internacionales de datos es necesaria una decisión de adecuación previa de la Comisión Europea, o bien que la entidad exportadora cumpla con garantías de protección adecuadas, salvo que se ampare en alguno de los supuestos de excepción que se prevén en el apartado 3 de este módulo. A estos efectos, se examinan las condiciones mediante las que una compañía u organización privada ubicada en territorio europeo puede transferir datos a terceros Estados u organizaciones internacionales, aunque estos no cumplan con las condiciones de adecuación establecidas por la Comisión Europea.

Finalmente, se analiza el marco legal aplicable a las transferencias internacionales por parte de un responsable de tratamiento ubicado en un Estado miembro de la UE; se va a estudiar más concretamente el caso de Estados Unidos, que suscribió dos acuerdos internacionales que permiten la transferencia de datos de la UE al territorio estadounidense.

1. Marco legal aplicable

El flujo transfronterizo de datos es imprescindible en la actualidad, ya que aumenta cada día. El derecho de la Unión Europea en materia de protección de datos pretende, principalmente, garantizar la libre circulación de datos en el mercado interior mediante la armonización de la normativa de la UE. Por regla general, se prohíbe la transferencia de datos a terceros países que no ofrezcan un nivel adecuado de protección.

Sin embargo, intentar bloquear o restringir sin razón alguna tales flujos, con el fin de garantizar una protección de datos adecuada, puede estar abocado al fracaso. Por ello, la prohibición no obstaculiza las transferencias que respetan determinados requisitos legales –la normativa de la UE reconoció ya en 1995, en la Directiva 95/46/CE de Protección de Datos (DPD), la importancia del proceso de globalización cada vez mayor–. El régimen de las transferencias internacionales regulado por la DPD ha funcionado durante treinta años, pero a causa de los rápidos progresos tecnológicos, su clausulado ha quedado obsoleto y ha requerido de actualización.

Tras las revelaciones hechas por Edward Snowden sobre las prácticas de vigilancia de Estados Unidos, las soluciones ofrecidas por la normativa de la UE para permitir las transferencias transfronterizas de datos están ahora bajo estrecho control por el TJUE.

El TJUE destacó en 2015 la existencia de una serie de fragilidades significativas en el marco legal que existía hasta entonces (Puerto Seguro), concretamente en el asunto Schrems[1], el cual se analizará más adelante.

(1)Asunto C-362/14 Maximillian Schrems contra Data Protection Commissioner, de 6 de octubre de 2015.

Es esencial reconciliar la salvaguardia del derecho fundamental a la protección de datos con las transferencias internacionales eficaces de datos, que puedan contribuir válidamente al crecimiento y los nuevos modelos digitales cada vez más transfronterizos.

En cuanto a la legislación a tener en cuenta en transferencias internacionales de datos, tanto la DPD como el Reglamento general de protección de datos (RGPD) contienen disposiciones que establecen los requisitos para la transferencia de datos personales a terceros países u organizaciones internacionales. Así, el artículo 45(1) del RGPD establece que:

> «[p]odrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión 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».

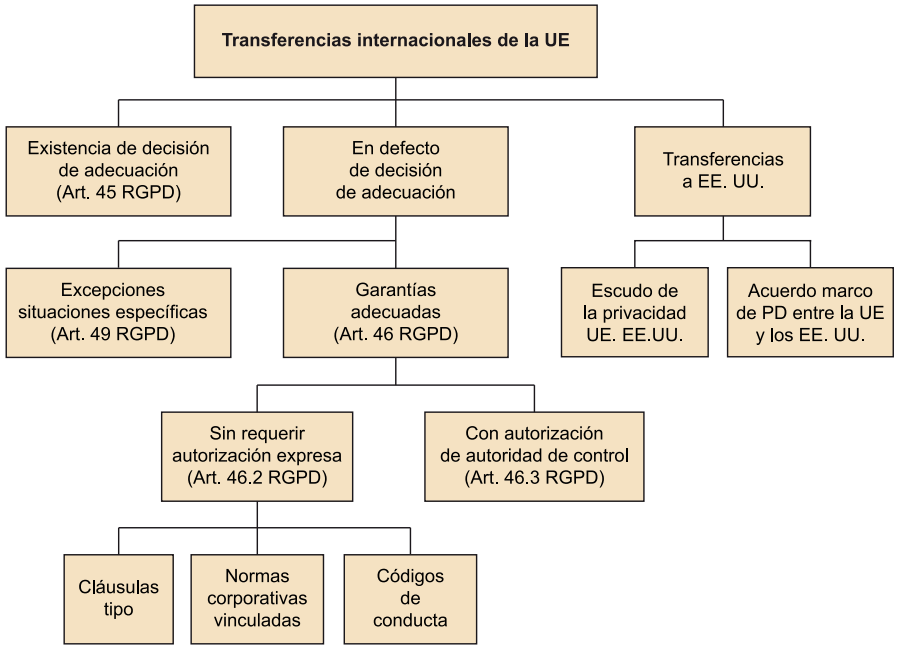
En cambio, la antigua Directiva del 95 solo dedicaba dos artículos a las transferencias internacionales: el 25 y el 26. El antiguo artículo 25 establecía, como principio general de régimen de transferencias internacionales, que estas únicamente eran posibles si el país tercero garantizaba un nivel de protección de datos adecuado. En otro caso, la transferencia estaría prohibida salvo que se diera alguna de las excepciones que enumeraba el antiguo artículo 26, entre las que se encontraba que el responsable del tratamiento ofreciera garantías suficientes de protección de derechos de los afectados.

El TJUE se encargó de concretar el alcance e interpretación del antiguo artículo 25 de la DPD mediante su jurisprudencia. Por ejemplo, en el caso Lindquist (C-101/01, 6 de noviembre de 2003), el TJUE decidió que no existe una «transferencia [de datos] a un tercer país» en el sentido del artículo 25 de la DPD cuando una persona de una Estado miembro cargue datos personales a una página de internet que se almacena en un dominio de internet en el que la página pueda ser consultada y que sea alojada por una persona física o jurídica establecida en dicho Estado o en otro Estado miembro, con lo que los datos quedan accesibles a toda persona que se conecte a internet, incluidas las personas de un tercer país (párrafo 71).

En el RGPD el modelo cambia con respecto a la antigua Directiva del 95, ya que se añade como supuesto admisible de legitimación de las transferencias, junto con la adecuación (art. 45), el del responsable o encargado que ofrezcan garantías adecuadas (art. 46), entre las que se encuentran las normas corporativas vinculantes (art. 47). De no darse alguna de estas dos circunstancias (adecuación o garantías), la transferencia será posible si se da alguna de las excepciones previstas para casos específicos (art. 49).

Ved también

Este punto se detalla en el apartado 3 de este módulo.



Según la Comisión Europea, los países que garantizan un nivel adecuado de protección son: Andorra, Argentina, Canadá, Islas Feroe, Guernesey, Israel, Isla de Man, Jersey, Nueva Zelanda, Suiza y Uruguay.

Además, la Comisión adoptó una Decisión sobre la adecuación del Puerto Seguro (Decisión 2000/520/CE de 26 de julio de 2000) con el Departamento de Comercio de Estados Unidos; consideraba que si se cumplían unos determinados principios de privacidad por las empresas estadounidenses, existía una protección adecuada para la transferencia de datos personales entre la UE y EE. UU. Sin embargo, el 6 de octubre de 2015, la Decisión de la Comisión fue declarada inválida por el Tribunal de Justicia de la Unión Europea en la sentencia Schrems (C-362/14).

En cuanto a las Decisiones de Adecuación de la Comisión Europea, la adecuación respecto la protección de datos en un tercer país implica que los principios fundamentales de la DPD y del nuevo RGPD son aplicados de forma efectiva en la legislación nacional de ese país, debido a su legislación interna o a los compromisos internacionales que dicho tercer país ha contraído.

Las Decisiones de Adecuación de la Comisión Europea son jurídicamente vinculantes para los Estados miembros y para los Estados del EEE. El requisito de adecuación, más que la equivalencia, lo que permite es el respeto de las diferentes formas de aplicar la protección de datos.

Según la DPD, las propuestas de las Decisiones de Adecuación de la Comisión estaban sujetas al Dictamen de las autoridades de protección de datos de los Estados miembros y del Supervisor Europeo de Protección de Datos (SEPD), en el marco del Grupo de Trabajo del Artículo 29, y a la aprobación del Comité del Artículo 31, integrado por representantes de los Estados miembros, en el marco de comitología. En cualquier momento, el Parlamento o el Consejo podían solicitar a la Comisión que mantuviera, modificara o retirara una Decisión de adecuación por considerar que excedía de las competencias de ejecución concedidas por la DPD.

En cambio, según el RGPD, la Comisión es la única institución competente para emitir decisiones de adecuación. Según el artículo 45 del RGPD, en sus decisiones de adecuación, la Comisión debe establecer un mecanismo para revisar de manera periódica su aplicación. Dicha revisión debe llevarse a cabo en colaboración con el tercer país u organización internacional de que se trate y tener en cuenta todos los cambios en la materia que se produzcan en dicho tercer país u organización internacional. Por ello, tras haber evaluado la adecuación del nivel de protección, la Comisión puede decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado. Dicho acto de ejecución se adoptará con arreglo al procedimiento de examen al que se refiere el artículo 93.2 del RGPD, que a su vez se remite al artículo 5 del Reglamento (UE) núm. 182/2011 del

Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión. Pero junto con la Comisión, el Comité Europeo de Protección de Datos tiene un papel importante en el procedimiento, ya que facilitará a la Comisión un dictamen para evaluar la adecuación de un nivel de protección de datos en un tercer país u organización internacional, en particular para evaluar si un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o una organización internacional, ya no garantizan un nivel de protección adecuado. Con el fin de realizar ese dictamen, la Comisión facilitará al Comité toda la documentación necesaria, incluida la correspondencia con el gobierno del tercer país.

Además del RGPD, cabe destacar el Convenio del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de datos personales (Convenio núm. 108). Este convenio tiene por objeto garantizar «en el territorio de cada parte para cada individuo [...] el respeto de sus derechos y libertades fundamentales, y en particular su derecho a la privacidad, en lo que respecta al tratamiento automatizado de los datos personales que le conciernen». El artículo 12.2 y 3 del Convenio permite a cada parte contratante transferir datos a una parte no contratante únicamente si el Estado u organización destinatario garantiza un nivel adecuado de protección para la transferencia de datos prevista.

El Protocolo Adicional (PA) al Convenio núm. 108 relativo a las autoridades de control y a las transferencias transfronterizas de datos permite las transferencias cuando no exista una protección adecuada de los datos, siempre que las transferencias estén previstas por el derecho interno y sean necesarias para los intereses específicos del interesado o concurran intereses legítimos prevalecientes de terceros, especialmente los intereses públicos esenciales.

2. Transferencias internacionales con países que no aseguren un nivel adecuado de protección

De todo lo anterior se puede deducir que será posible una transferencia internacional a un tercer país u organización internacional cuando la transferencia:

- se base en una decisión de adecuación,
- se base en garantías adecuadas,
- se base en alguna de las excepciones previstas en el artículo 49 del RGPD.

Así pues, tanto la anterior DPD como el actual RGPD (y también el Protocolo Adicional al Convenio núm. 108) permiten a la legislación nacional establecer regímenes para la transferencia transfronteriza de datos a terceros «países que no aseguren un nivel adecuado de protección» si:

- el responsable del tratamiento ha adoptado disposiciones especiales para garantizar que el destinatario disponga de las garantías adecuadas en materia de protección de datos; y
- el responsable puede probar dichas garantías ante la autoridad competente.

En este sentido, el artículo 46.2 del RGPD establece que se considerarán garantías adecuadas sin que requiera la autorización expresa de una autoridad de control:

- todo instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
- las cláusulas tipo de protección de datos adoptadas por la Comisión;
- las cláusulas tipo de protección de datos adoptadas por la autoridad de control y aprobadas por la Comisión;
- las normas corporativas vinculantes;
- los códigos de conducta vinculantes y exigibles del responsable o el encargado del tratamiento;
- otros mecanismos de certificación vinculantes y exigibles del responsable o el encargado del tratamiento.

2.1. Cláusulas contractuales tipo

Respecto a las cláusulas tipo, estas tienen sin duda notable relevancia. Se trata de cláusulas sobre transferencias entre responsables, encargados y subencargados. Son cláusulas que pueden ser adoptadas por la Comisión o por una autoridad de control[3] (en cuyo caso no es necesaria autorización alguna) o aportadas por las partes y autorizadas por una autoridad de control[2].

(2)En ese caso se aplicará el mismo mecanismo de coherencia, establecido en los artículos 46.4 y 64.1.e) del RGPD.

(3)En el artículo 58.3.g) del RGPD se especifica el poder de las autoridades de control para adoptar las cláusulas. Además, el artículo 64.1.d) dispone que el dictamen del Comité Europeo es obligatorio respecto de las cláusulas tipo de protección de datos adoptadas por una autoridad competente.

Según el artículo 46.5 del RGPD, las autorizaciones otorgadas por un Estado miembro o una autoridad de control, y las decisiones adoptadas por la Comisión en virtud del antiguo artículo 26.4 de la Directiva del 95 seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por la autoridad de control o por una decisión de la Comisión.

Actualmente, existen dos instrumentos que regulan **cláusulas contractuales tipo** que están oficialmente certificadas por una decisión de la Comisión como prueba de que existen las garantías adecuadas:

- La Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001 (modificada por la Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004), que regula las transferencias de un responsable (UE) a otro responsable (de fuera de la UE/EEE).

- La Decisión 2010/87/UE (por la que se deroga la Decisión 2002/16/CE), que regula las transferencias de un responsable (UE) al encargado (de fuera de la UE/EEE).

Las cláusulas contractuales tipo contienen una declaración jurídicamente exigible en virtud de la cual tanto el «exportador de datos» como el «importador de datos» se comprometen a tratar los datos de conformidad con las normas básicas de protección de datos (es decir, el respeto de la privacidad y los derechos y libertades fundamentales de los individuos) y están de acuerdo en que los interesados puedan ejercitar sus derechos en virtud del contrato.

Las cláusulas contractuales tipo pueden incluirse en un contrato más amplio y no impiden que los responsables adopten sus propias cláusulas *ad hoc*, siempre que garanticen un nivel idéntico de protección.

Sus características más importantes son:

- Una cláusula de terceros beneficiarios que permita a los interesados ejercer derechos contractuales aunque no sean parte en el contrato.

- El destinatario o importador de datos acuerda someterse al procedimiento de la autoridad nacional de control del Estado del responsable de la exportación de datos y/o a los tribunales en caso de conflicto.

2.2. Normas Corporativas Vinculantes

Una de las más importantes novedades del RGPD es la referencia y detallada regulación que se hace de las **Normas Corporativas Vinculantes** (NCV).

Las NCV están expresamente reguladas en el artículo 47 del RGPD y son un conjunto de normas aplicables de forma voluntaria sobre un grupo multinacional de empresas, a modo de código de conducta, que define la manera en que las transferencias internacionales de datos operan dentro del grupo. El reglamento las define como

> «políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta».

Una vez aprobadas, las transferencias de datos dentro del grupo multinacional a países que no ofrecen un nivel adecuado de protección se considerarán que sí ofrecen las garantías adecuadas.

Todas las autoridades de protección de datos implicadas deben incorporar el resultado de la evaluación en sus procedimientos formales de concesión de las autorizaciones.

El Grupo de Trabajo del Artículo 29 ha publicado tres documentos en los que se concretan los requisitos sobre las NCV que las empresas deben cumplir:

- El Documento de Trabajo que establece un marco para la estructura de Normas Corporativas Vinculantes (GT 154, 2008).

- El Documento de Trabajo que establece una lista de verificación a modo de solicitud modelo para la aprobación de las Normas Corporativas Vinculantes (GT 108, 2005).

- El Documento de Trabajo que establece una lista con los elementos y los principios que se encuentran en las Normas Corporativas Vinculantes (GT 153, 2008).

El contenido obligatorio de las NCV establecido por los Documentos de Trabajo del GT29 garantiza su carácter vinculante y su aplicabilidad jurídica.

Aunque las NCV fueron inicialmente concebidas para transferencias entre responsables del mismo grupo multinacional de empresas, el Grupo de Trabajo del Artículo 29 publicó en 2012 las Normas Corporativas Vinculantes para transferencias dentro de un grupo de empresas encargadas del tratamiento (GT 204, 2013, revisado en 2015), que son reglas especialmente adecuadas para las multinacionales encargadas de la computación en la nube, por ejemplo.

El artículo 47.1 del RGPD establece los requisitos que deben tener las NCV de conformidad con el mecanismo de coherencia:

a) que sean jurídicamente vinculantes y que se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) que confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales; y

c) que cumplan con el contenido mínimo que prevé el apartado 2 del artículo 47, que deberá incluir:

- la descripción de la estructura del grupo y datos de contacto de cada uno de sus miembros, así como las transferencias o conjuntos de transferencias de datos, categorías de datos, tipos de interesados afectados, tipo de tratamientos, fines y países de destino.

- Un contenido jurídico-sustancial de gran calado con carácter jurídicamente vinculante de las normas, la aplicación de los principios de protección de datos, los derechos de los afectados y medios para ejercerlos en los Estados miembros, la aceptación de responsabilidad por actuación de miembros no establecidos en la UE, los procedimientos de reclamación, y la forma de informar sobre las NCV a los interesados.

- Las funciones del delegado de protección de datos o cualquier persona o entidad encargada de la supervisión del cumplimiento de las normas.

- Mecanismos para garantizar la verificación del cumplimiento (por ejemplo, auditorías o acciones correctivas).

- Mecanismos para la modificación de las normas y notificación a la autoridad de control, mecanismos de cooperación e información a las autoridades de control, mecanismos para informar a la autoridad de cualquier

requisito jurídico en el país tercero que pueda tener efecto adverso en las normas.

- La formación recibida por el personal en temas de protección de datos.

El **procedimiento de aprobación** es el siguiente. En primer lugar, para cada NCV, una autoridad de protección de datos líder debe ser nombrada por el grupo corporativo para dirigir el procedimiento de la aprobación. La solicitud de autorización de la NCV debe realizarse en los Estados miembros de la sede de la organización, salvo en el caso de que estos se encuentren fuera de la UE, en cuyo caso deberá efectuarse en el Estado miembro en el que el grupo tenga un miembro. A continuación, la autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia, mediante el cual el Comité Europeo de Protección de Datos podrá emitir un dictamen previo (art. 64 RGPD). Las autoridades de control de los países miembros del EEE donde están establecidas las filiales del grupo son invitadas, por el órgano de control, a participar voluntariamente en el proceso de evaluación de las NCV. Finalmente, se deberá designar una persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones (art. 47.2.h) del RGPD).

La UE y el Foro de Cooperación Económica Asia-Pacífico están trabajando en la interoperabilidad o el reconocimiento mutuo entre las NVC de la UE y los sistemas de Reglas sobre la Privacidad Transfronteriza (CBPR por sus siglas en inglés) del Foro de Cooperación Económica Asia-Pacífico (Carson, 2015).

Referencia bibliográfica

Angelike Carson (2015, 26 de mayo). «EU and APEC Officials agree to streamline BCR/CBPR application process». IAPP. Accesible en: https://iapp.org/news/a/eu-and-apec-officials-agree-to-streamline-bcrcbpr-application-process/.

2.3. Códigos de conducta y garantías *ad hoc*

Como novedad del RGPD, las transferencias a terceros países podrán autorizarse sobre la base de **códigos de conducta** o mecanismos de certificación aprobados, siempre que el responsable o el encargado del tratamiento en el tercer país suscriba los compromisos vinculantes y ejecutables que establezcan las garantías apropiadas, incluidas las relativas a los derechos de los interesados.

Así mismo, podrán acordarse garantías *ad hoc*, previa autorización de la autoridad de control competente y de un mecanismo de coherencia, a fin de garantizar la aplicación coherente del RGPD en la UE.

2.4. Otras excepciones

Tal y como se recogía en la Directiva del 95 en su artículo 26, el RGPD dedica un epígrafe a «excepciones para situaciones específicas». Según el artículo 49.1 del RGPD (Piñar, 2016), la transferencia de datos de terceros países en ausencia de una constatación de la adecuación es permitida si:

- El interesado ha dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos.
- La transferencia es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento.
- La transferencia es necesaria para la celebración o ejecución de un contrato, en interés del interesado.
- La transferencia es necesaria por razones importantes de interés público.
- La transferencia es necesaria para la formulación, el ejercicio o la defensa de reclamaciones.
- La transferencia es necesaria para proteger los intereses vitales del interesado.
- La transferencia se realiza desde un registro público que tiene por objeto facilitar información al público y está abierto a la consulta del público o de una persona con un interés legítimo.

Las situaciones a las que se refiere el artículo 49 constituyen un supuesto de *numerus clausus*, es decir, es una lista cerrada, de modo que no puede aplicarse ninguna otra por analogía. Sin embargo, algunas de ellas son excesivamente amplias y el último párrafo del artículo 49.1, como novedad del RGPD, admite las transferencias cuando no sea aplicable ninguna de las excepciones en él enumeradas, siempre que: a) no sea repetitiva, b) afecte solo a un número limitado de interesados, c) sea necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos del interesado, d) y el responsable del tratamiento haya evaluado todas las circunstancias concurrentes en la transferencia de datos y cumpla con las garantías suficientes de protección de datos personales.

Estas excepciones amplían las ya contenidas en el antiguo artículo 26.1 de la DPD. Sobre la base de ese artículo, el Grupo de Trabajo del Artículo 29 publicó una Guía relativa a la interpretación de las excepciones titulada «Documento de Trabajo sobre una interpretación común del artículo 26, apartado 1, de la Directiva de Protección de Datos de 24 de octubre de 1995». En él se especifi-

Referencia bibliográfica

Para un análisis más detallado, ver:

Jose Luis Piñar Mañas (2016). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 454-456). Editorial Reus.

caba que dichas excepciones debían ser interpretadas restrictivamente y que debían aceptarse únicamente en los casos en que no podía aplicarse el apartado 2 del artículo 26 sobre las cláusulas contractuales tipo.

Si se da alguna de estas excepciones, el responsable del tratamiento debe informar a la autoridad de control y a los interesados sobre la transferencia y sobre los intereses legítimos perseguidos.

El mayor inconveniente de algunas de las excepciones del artículo 49, en relación con las cláusulas tipo de la Comisión Europea, es que no garantizan la protección una vez que los datos se han exportado, mientras que las cláusulas tipo de la Comisión se aplican durante todo el tiempo en que perdura el contrato y, por lo tanto, se mantienen después de que los datos ya se hayan exportado al tercer país.

3. Escudo de la Privacidad UE-EEUU

Actualmente, el Escudo de la Privacidad EU-EEUU, que se aprobó formalmente el 12 de julio de 2016[4], ha sustituido los principios de privacidad del anterior Puerto Seguro tras el asunto Schrems del TJUE. Los principios de privacidad del Puerto Seguro se incluían en un acuerdo, en forma de código de conducta entre la UE y Estados Unidos, que era aplicable a las empresas estadounidenses, supervisadas por la Comisión Federal del Comercio de los Estados Unidos. Se puso a disposición en línea una lista de organizaciones que se sumaron voluntariamente a los principios de Puerto Seguro mediante compromisos y sistemas de autocertificación. Tales principios eran vinculantes para las empresas que se adherían a ellos.

[(4)]C(2016) 4176 final, «Commission Implementing Decision of 12.7.2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield».

La Decisión 2000/520/CE de la Comisión Europea consideró que este régimen garantizaba un nivel adecuado de protección de los datos personales transferidos; pero dicha decisión fue invalidada por el TJUE en el asunto Schrems.

Schrems es un estudiante austríaco de Derecho que presentó una denuncia ante el Comisario de Protección de Datos de Irlanda contra Facebook Ireland Limited, la filial irlandesa de dicha empresa, responsable de todas las cuentas pertenecientes a usuarios fuera de Norteamérica (contabilizando el 80 % de 1,35 millones de usuarios de Facebook) y que está sujeta a la legislación europea.

El Comisario desestimó la denuncia europea interpuesta por presuntos incumplimientos de la normativa de privacidad de la UE, por la vigilancia masiva y por análisis intrusivos realizados por la Agencia de Seguridad nacional de Estados Unidos. Se consideró que, con arreglo al sistema de Puerto Seguro, Estados Unidos garantizaba un nivel adecuado de protección.

El caso fue recurrido ante el Tribunal Supremo de Irlanda, que suspendió el procedimiento y remitió una cuestión prejudicial al TJUE.

De hecho, la adecuación del Acuerdo de Puerto Seguro ya fue cuestionado en una Comunicación de la Comisión de 2013 (COM(2013)847 final). La Comisión identificó las siguientes deficiencias relativas al sistema de Puerto Seguro que debían ser tratadas:

- La falta de transparencia de las políticas de privacidad de los miembros del sistema de Puerto Seguro.

- La aplicación efectiva de los Principios de Privacidad por parte de las empresas en Estados Unidos.

- La efectividad de la aplicación.

- El acceso a gran escala por parte de las agencias de inteligencia a los datos transferidos a Estados Unidos por las empresas certificadas por el sistema de Puerto Seguro.

La crítica principal fue que el sistema de Puerto Seguro era demasiado permisivo al acceso de terceros a los datos personales en Estados Unidos, incluyendo el acceso por el Gobierno estadounidense.

La existencia de una decisión de la Comisión que declare que un tercer país garantiza un nivel adecuado de protección de los datos personales transferidos no puede eliminar, ni siquiera reducir, las facultades de que disponen las autoridades nacionales de control en virtud de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE).

Así, en el asunto C-362/14 de Maximilian Schrems contra la Comisión de Protección de Datos, el Tribunal estableció que la CDFUE y la DPD no prevén limitaciones a las competencias de las autoridades nacionales de control sobre las transferencias de datos a terceros países y, en consecuencia, la Comisión «no tiene competencia para limitar las competencias de las autoridades nacionales de control».

Por ello, el TJUE acabó determinando que la decisión de adecuación de la Comisión Europea sobre el sistema de Puerto Seguro era inválida, ya que:

- los «requisitos de seguridad nacional, de interés público y de aplicación de la ley» de Estados Unidos prevalecen sobre el sistema de Puerto Seguro, permitiendo «ignorar, sin limitaciones, las normas de protección establecidas por el sistema en caso de conflicto»;

- el consecuente acceso generalizado por las autoridades públicas de Estados Unidos «al contenido de las comunicaciones electrónicas debe ser entendido como que dicho acceso compromete la esencia del derecho fundamental al respecto de la vida privada»;

- la falta de disposiciones en el sistema de Puerto Seguro «que permite que un individuo pueda ejercer los recursos jurídicos para tener acceso a los datos personales que le conciernen o para obtener la rectificación o la cancelación de dichos datos compromete la esencia del derecho fundamental a un recurso judicial efectivo».

A raíz de esta decisión, el Grupo de Trabajo del Artículo 29 (GT29) declaró que la sentencia del Tribunal exigía que toda decisión de adecuación implicaba un amplio análisis de las leyes nacionales de los países terceros y de los compromisos internacionales[5]. Por ello, el Grupo de Trabajo recomendaba lo siguiente:

(5)Statement of the Article 29 Working Party, 16th October 2015:http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

- Los Estados miembros y la Comisión Europea deberían entablar un debate con las autoridades estadounidenses «para encontrar soluciones políticas, jurídicas y técnicas que permitan realizar transferencias de datos al territorio de Estados Unidos que respeten los derechos fundamentales».

- Una posible solución parcial es un nuevo Puerto Seguro, como un acuerdo intergubernamental que ofrezca garantías más sólidas a los interesados de la UE mediante mecanismos vinculantes que «limiten el control necesario del acceso de las autoridades públicas, la transparencia, la proporcionalidad, los recursos y los derechos de la protección de datos».

En noviembre de 2015, el GT29 decidió que, si a finales de enero de 2016 no se llegaba a una solución adecuada con las autoridades estadounidenses, y dependiendo de la evaluación de los instrumentos de transferencia por el Grupo de Trabajo, las autoridades de protección de datos de la UE se comprometerían a tomar todas las medidas necesarias y apropiadas.

El Escudo de la Privacidad UE-EEUU[6] mantiene la misma metodología que el antiguo Acuerdo de Puerto Seguro. Así pues, las empresas privadas pueden registrarse voluntariamente en el Escudo de la Privacidad si autocertifican que cumplen con las condiciones requeridas. Las organizaciones estadounidenses se comprometen a un conjunto de principios de privacidad que son emitidos por el Departamento de Comercio de Estados Unidos (en adelante, Principios). Los Principios se aplican tanto a los responsables como a los encargados (agentes), con la especificidad de que los encargados deben estar obligados contractualmente a actuar solo de acuerdo con las instrucciones del responsable de la UE y ayudar a estos a responder a las personas que ejerzan sus derechos conforme a tales Principios.

(6)Documento accesible en:https://www.privacyshield.gov/servlet/ servlet.FileDownload?file=015t00000004qAg

Por lo tanto, se permiten las transferencias de un responsable o encargado en la UE a organizaciones en Estados Unidos que han autocertificado su adhesión a los Principios a través del Departamento de Comercio y se han comprometido a cumplir con ellos.

Es aplicable también a los países del EEE (Islandia, Liechtenstein y Noruega) después de que el Comité Mixto del EEE decidiera sobre la incorporación de la Decisión sobre el Escudo de Privacidad UE-EEUU al Acuerdo EEE. Los interesados de la UE cuyos datos personales sean transferidos a organizaciones esta-

dounidenses que hayan autocertificado su adhesión a los Principios a través del Departamento de Comercio (en adelante, DoC) se benefician de la protección ofrecida por el Escudo de Privacidad UE-EEUU.

No obstante, para controlar este mecanismo, el Escudo de la Privacidad incorpora algunas novedades. Por ejemplo, las condiciones de registro son más estrictas que las del Puerto Seguro, ya que requieren la confirmación del DoC obligatoriamente para poder completar la solicitud. Finalmente, las empresas que se unen al Escudo de la Privacidad se verán sujetas a auditorías periódicas para verificar que siguen cumpliendo con las condiciones iniciales. Por lo tanto, las autocertificaciones se deben renovar cada año, mientras que el anterior Puerto Seguro no: una vez que la empresa se incluía en la lista, la autocertificación no tenía fecha de caducidad.

Se ven reforzados aspectos como el hecho de que los Principios del nuevo Escudo de la Privacidad incluyen condiciones que no se encontraban en el Puerto Seguro pero que están presentes en el Reglamento general de protección de datos (RGPD). Así, por ejemplo, en el anterior acuerdo, las transferencias ulteriores no estaban prohibidas y los datos podían seguir transfiriéndose, una vez se mandaban a la empresa estadounidense, sin el consentimiento del usuario (a los ciudadanos europeos se les daba la posibilidad de oponerse a dicho tratamiento solamente en casos muy puntuales). En cambio, el Escudo de la Privacidad solo permite la transferencia ulterior de datos para fines muy específicos, y los encargados del tratamiento del tercer país quedarán obligados a garantizar la misma protección de datos que la establecida en el Escudo de la Privacidad, y serán responsables junto con los responsables del tratamiento en caso de producirse una vulneración de la privacidad.

Aun así, hay algunos aspectos en el nuevo acuerdo que se han recibido con cierta decepción por parte de los sectores que defienden la protección de datos. Por ejemplo, el Parlamento Europeo lamenta que el nuevo acuerdo aún se fundamenta en la autocertificación y no implementa un mecanismo de registro más estricto[7]. Además, el nuevo texto sigue sin contener normas precisas sobre la recogida masiva de datos, y tampoco incluye salvaguardas robustas de supervisión y recursos efectivos para posibles lesiones del derecho de protección de datos a ciudadanos europeos[8].

(7)Parlamento Europeo, Resolución del Parlamento Europeo, de 6 de abril de 2017, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EEUU (2016/3018(RSP)), punto 2.

(8)Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre los flujos transatlánticos de datos (2016/2727(RSP)), párrafo 13.

El Escudo de la Privacidad prevé un sistema compuesto por varias capas para la resolución de litigios administrativos. En concreto, la Comisión Federal de Comercio de Estados Unidos (en adelante, FTC, por sus siglas en inglés), el DoC, el Defensor del Pueblo (*Ombudsperson*) del Escudo de la Privacidad, y las autoridades de protección de datos de los Estados miembros ofrecen procedimientos simultáneos para la resolución de conflictos.

Anteriormente, con el sistema de Puerto Seguro, solamente había un mecanismo de solución de litigios en caso de una violación de protección de datos. El artículo 5 de la Ley de FTC preveía que la FTC era la única autoridad competente en caso de que las empresas empleasen métodos de competencia desleales o bien prácticas, y actos desleales o fraudulentos, que afectaran al comercio. Sobre la base del Escudo de la Privacidad, la FTC continúa aplicando estas sanciones, pero puesto que no puede ser considerada como una autoridad de supervisión independiente, se han introducido otros mecanismos adicionales.

Concretamente, el Escudo de la Privacidad ofrece los cuatro mecanismos de cumplimiento que se han mencionado anteriormente: a) acudir a la autoridad de protección de datos del país del afectado; b) acudir a la FTC; c) acudir al DoC; d) y acudir al *Ombudsperson* del Escudo de la Privacidad.

En primer lugar, los ciudadanos europeos pueden interponer una queja a la compañía misma, y esta tiene 45 días para dar una respuesta y resolver el problema. Sin embargo, si la vulneración por parte de una compañía estadounidense registrada en el Escudo de la Privacidad subsiste, los ciudadanos europeos tienen un mecanismo alternativo a través de un panel de autoridades de protección de datos establecido en la UE. Este mecanismo se creó con el fin de cumplir con la sentencia del TJUE en el asunto Schrems. El Tribunal concluyó que las autoridades de protección de datos debían poder resolver casos de incumplimiento de normas de protección de datos por parte de empresas estadounidenses. Por ello, en el nuevo acuerdo, las autoridades nacionales de protección de datos –a veces con la asistencia del DoC y de la FTC[9]– proporcionan un mecanismo de recurso independiente que permite investigar quejas contactando con la empresa y buscando la medida compensatoria más justa. Este procedimiento puede durar hasta 60 días desde el día en que la autoridad nacional de protección de datos recibe la queja. A continuación, la compañía tiene 25 días para cumplir con la recomendación que reciba[10]. No obstante, no queda claro cómo deben cooperar las autoridades de protección de datos entre ellas en la práctica[12]. ¿Interactuarán en un único panel o se constituirán en paneles diferentes dependiendo del caso? Este punto no queda claro en el articulado del acuerdo, aunque el Grupo del Artículo 29 ha publicado una guía, en este sentido, en la que se definen más concretamente el sistema de evaluación y la composición de los paneles de autoridades de protección de datos, así como el formulario a rellenar en caso de vulneración de alguno de los artículo del Escudo de la Privacidad[11].

(9)U.S. SAFE WEB Act of 2006, Pub. L. 109-455, 22 de diciembre de 2006.

(10)Escudo de la Privacidad, Considerando 49.

(11)Grupo del Artículo 29, «Rules of Procedure for the «Informal Panel of EU DPAs» According to the EU-US Privacy Shield» y «Complaint Form for Submitting Commercial Related Complaints to EU DPAs», 21 de febrero de 2017.

(12)Grupo del Artículo 29, «Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decisión», WP 238, 13 de abril de 2016, pág. 27; Supervisor Europeo de Protección de Datos, «Opinion on the EU-US Privacy Shield draft adequacy decisión», Opinión 4/2016, 30 de mayo de 2016, pág. 10.

Si el mecanismo de las autoridades de protección de datos no resuelve el caso, los ciudadanos europeos pueden optar por otros recursos que se llevarán a cabo en territorio estadounidense. Si esto sucede, la autoridad nacional de protección de datos va a canalizar la queja al DoC y a la FTC, los cuales ini-

(13)Escudo de la Privacidad, Considerando 52.

ciarán una investigación que puede durar hasta 90 días[13]. Los procedimientos del DoC y la FTC en el Escudo de la Privacidad son diferentes de los del antiguo sistema de Puerto Seguro, ya que en este último el DoC tenía la exclusividad en la detección de certificaciones falsas de las compañías registradas. Si se identificaba alguna falsedad, el DoC mandaba una carta de advertencia a la compañía y la FTC podría tomar acciones legales contra ella.

Con el Escudo de la Privacidad, las funciones del DoC se ven reforzadas. Este órgano ha aumentado el número de personas que forman parte de su equipo precisamente con el fin de cumplir con los principios establecidos, incluyendo mecanismos efectivos de control, así como sanciones y supresión de las empresas de la lista de registro. El DoC verifica continuamente las compañías que se autocertifican mediante cuestionarios detallados que dichas compañías deben responder, y si no dan una respuesta satisfactoria o bien el DoC detecta una afirmación falsa de participación en el Escudo de la Privacidad, entonces se inicia una investigación y puede llegarse a suprimir la empresa del listado del Escudo de la Privacidad si se verifica que no cumple con los principios del sistema. Una vez eliminada la compañía del registro, esta debe comprometerse a devolver o destruir todos los datos personales obtenidos bajo el sistema del Escudo de la Privacidad, y una lista de «señale y denuncie» para estas compañías quedará visible en la página web de la FTC.

Además, el DoC puede suprimir de la lista todas esas compañías que voluntariamente decidan salir del Escudo de la Privacidad. Si este es el caso, el DoC se reserva la opción de mandar cuestionarios a dichas empresas para conocer los motivos por los cuales decidieron finalizar su registro en el sistema.

Un último mecanismo a mencionar es en el que interviene el Defensor del Pueblo u *Ombudsperson*. Aunque la figura del Defensor del Pueblo lleva existiendo en los diferentes Estados miembros de la UE desde los años cincuenta, este órgano es completamente novedoso en el sistema jurídico de Estados Unidos. El *Ombudsperson* del Escudo de la Privacidad se ha nombrado por el Departamento del Estado de Estados Unidos y se encarga de examinar posibles vulneraciones de los derechos de privacidad y protección de datos por parte de las autoridades estadounidenses. El *Ombudsperson*, para ejecutar sus funciones, debe tener conocimiento de las actividades que realizan tanto agentes de policía como servicios de inteligencia de Estados Unidos. También revisará las quejas que se interpongan ante estos organismos públicos, realizando funciones de intermediario entre el usuario y las agencias de seguridad estadounidenses.

Sin embargo, se pone en cuestión la independencia y falta de poderes del *Ombudsperson* en la práctica. Si se compara con los Defensores del Pueblo en los distintos Estados miembros, se puede ver que su papel se basa en emitir re-

comendaciones y orientaciones generales, basándose principalmente en conseguir el cambio mediante la presión social y política, no siendo estos actos vinculantes desde el punto de vista jurídico.

Según la Comisión Europea, el Escudo de Privacidad UE-EEUU impone obligaciones más fuertes a las empresas estadounidenses respecto a los datos personales de los europeos. Además, refleja los requisitos del TJUE, que declaró nulo el anterior sistema de Puerto Seguro.

El Escudo de Privacidad de la UE y Estados Unidos obliga a Estados Unidos a controlar y hacer cumplir de manera más sólida y a cooperar más con las autoridades europeas de protección de datos. Incluye, por primera vez, los compromisos escritos y las garantías de acceso a los datos por parte de las autoridades públicas. Estados Unidos garantiza por escrito que cualquier acceso de las autoridades públicas a los datos personales estará sujeto a claras limitaciones, garantías y mecanismos de control. Las autoridades de Estados Unidos afirman la ausencia de vigilancia indiscriminada o masiva.

El 26 de julio de 2016[14], el Grupo de Trabajo del Artículo 29 emitió una declaración en la que acogía con beneplácito las mejoras introducidas por el mecanismo del Escudo de Privacidad entre la UE y Estados Unidos en comparación con la decisión sobre el Puerto Seguro, pero también expresó una serie de preocupaciones relativas tanto a aspectos comerciales como al acceso a los datos por parte de las autoridades públicas estadounidenses.

(14)Accesible en:http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf

4. El Acuerdo Marco de protección de datos entre la UE y EEUU

Las revelaciones de Snowden demostraron que no solamente los entes privados pueden cometer vulneraciones del derecho de protección de datos, sino que los gobiernos también llevan a cabo prácticas que pueden ser contrarias al derecho de privacidad y protección de datos. Estas revelaciones aceleraron la necesidad de adopción de un acuerdo que estableciera límites en la recogida y tratamiento de datos de los ciudadanos europeos por parte de las agencias gubernamentales estadounidenses.

Por ello, además del Escudo de Privacidad de la UE y Estados Unidos, las transmisiones transatlánticas de datos están sujetas a las normas recogidas en el Acuerdo Marco de protección de datos UE-EEUU, cuando los datos personales intercambiados cumplen con los fines de prevención, investigación y enjuiciamiento de delitos, incluido el terrorismo.

Después de seis años de negociaciones, el 2 de junio de 2016, Estados Unidos y la UE firmaron el Acuerdo Marco de Protección de Datos entre la UE y los EEUU (en adelante, Acuerdo Marco[15]), el cual entró en vigor el pasado 1 de febrero de 2017. El Acuerdo Marco regula transferencias de datos entre las autoridades públicas de Estados Unidos y de la UE para la prevención, investigación, detección y persecución de delitos.

(15)Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences.

El objetivo principal de este acuerdo es ampliar los derechos de protección de datos de los ciudadanos europeos cuando sus datos son transferidos al gobierno de Estados Unidos con fines de seguridad. Sin embargo, se podrían resumir los objetivos en:

- Complementar los acuerdos vigentes entre la UE y Estados Unidos, así como entre los Estados miembros y Estados Unidos, relativos a las autoridades policiales.

- Armonizar las normas de protección de datos y establecer un alto nivel de protección para futuros acuerdos en este ámbito.

- Reconocer a los ciudadanos de la UE los mismos derechos y recursos judiciales que los reconocidos a los ciudadanos estadounidenses en caso de violación de la privacidad.

El Acuerdo Marco aumenta el nivel de protección de datos de los ciudadanos de la UE por las siguientes razones:

- Estableciendo los fines exclusivos para la transferencia: la prevención, la investigación, la detección o el enjuiciamiento de delitos penales, incluido el terrorismo, en el marco de la cooperación policial y la cooperación judicial en materia penal.

- Exigiendo que Estados Unidos solo pueda transferir los datos que recibió a un tercer país o a una organización internacional con el consentimiento previo de la autoridad competente de la UE que originalmente haya transferido los datos.

- Estipulando que los datos de los individuos no sean conservados por más tiempo del necesario o apropiado.

- Preconociendo, en ciertas circunstancias, a los interesados el derecho de acceso y rectificación.

Entre las agencias de gobierno receptoras de datos podemos encontrar autoridades policiales, judiciales y aduaneras localizadas en territorio de Estados Unidos y la UE. Por ejemplo, intercambios de datos entre Europol y la Oficina Federal de Investigación (FBI) quedarían sujetos a este acuerdo. Asimismo, si el departamento de policía alemán mandara datos personales relacionados con una investigación policial al departamento de policía de Nueva York, debería seguir las normas de este acuerdo. Sin embargo, conviene remarcar que los intercambios transatlánticos de datos por parte de servicios de inteligencia quedan excluidos del alcance del Acuerdo Marco.

El artículo 6.2 del Acuerdo Marco establece que el tratamiento de datos mediante este acuerdo es compatible con la regulación de los acuerdos internacionales existentes que también prevén la transferencia de datos con fines de prevención, detección, investigación y persecución de delitos. En otras palabras, se presume que acuerdos internacionales específicos con Estados Unidos como, por ejemplo, el Acuerdo sobre asistencia mutua[16], el de registro de pasajeros[17] o el que permite el intercambio de datos financieros[18] respetan los artículos del Acuerdo Marco. Así, los datos de pasajeros o la información financiera recogida por estos acuerdos específicos quedan cubiertos por el artículo 19.1 del Acuerdo Marco, según el cual se obliga a proporcionar compensación judicial a los ciudadanos europeos en caso de violación de sus derechos de protección de datos. Sin embargo, la adopción del Acuerdo Marco no afecta a otros acuerdos internacionales con Estados Unidos que no tienen como objetivo principal la prevención, detección, investigación y persecución de delitos, y por este motivo el Escudo de la Privacidad no tiene la obligación de respetar el clausulado del Acuerdo Marco o viceversa.

(16)Agreement on Mutual Legal Assistance between the United States of America and the European Union, 25 de Junio de 2003.

(17)Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, 14 de diciembre de 2011.

(18)Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, 13 de enero de 2010. DOUE L8/11.

El Acuerdo Marco (igual que el Escudo de la privacidad) incluye un serie de principios, entre los que se encuentran el principio de limitación de finalidad (art. 6), el principio de calidad e integridad de los datos (art. 8) y la cláusula de no discriminación. El artículo 7 del Acuerdo Marco establece la necesidad de un consentimiento previo de la primera autoridad, que envía los datos en caso de transferencias ulteriores, y se requiere que el tercer Estado que recibe la información garantice un nivel apropiado de protección de datos. Asimismo, los principios de proporcionalidad y necesidad se ven recogidos en el preámbulo del Acuerdo Marco. Finalmente, el Acuerdo Marco añade salvaguardas especiales para el tratamiento de datos sensibles (art. 13), así como una cláusula de conservación de datos que prevé que los datos personales no pueden almacenarse por más tiempo del necesario (art. 12). La inclusión de estos principios tiene una relevancia especial, ya que el TJUE ha subrayado en la sentencia Schrems que las autoridades policiales y judiciales no pueden recoger o tratar datos personales de los ciudadanos europeos si no es cumpliendo con los principios de proporcionalidad y necesidad, y sin excederse a la causa de su obtención.

Además de los requisitos establecidos por el TJUE, la Comisión Europea y las autoridades estadounidenses tuvieron otro obstáculo a la hora de confeccionar el Acuerdo Marco: debían armonizar dicho acuerdo con la Directiva 2016/680[19], recientemente adoptada. Esta Directiva regula cualquier intercambio de datos transfronterizo entre autoridades policiales y judiciales dentro de la UE, así como el tratamiento de datos personales entre entes policiales en el ámbito interno. Así pues, era imprescindible que cualquier acuerdo internacional relacionado con el intercambio de datos entre entes policiales y judiciales de la UE (como es el caso del Acuerdo Marco) fuera coherente con las normas de la UE y concretamente con la Directiva (UE) 2016/680.

(19)Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. DOUE L 119, 4 de mayo de 2016, págs. 89-131.

Uno de los mayores logros de este acuerdo es la inclusión de normas sobre transferencias ulteriores. Tal y como ya se ha mencionado, según el artículo 7, cualquier transferencia ulterior de datos más allá de territorio europeo y estadounidense requiere el consentimiento de la autoridad de protección de datos del país donde los datos provienen. Además, el artículo 16.4 establece que los ciudadanos europeos pueden autorizar a un organismo de control (que normalmente será la autoridad de protección de datos del país donde residen) para que lleve a cabo una petición de acceso en su nombre.

Finalmente, de acuerdo con la Directiva (UE) 2016/680, el Acuerdo Marco refuerza derechos de los ciudadanos europeos como: el derecho de acceso, rectificación, supresión y bloqueo de sus datos; un nuevo mecanismo de control; y el derecho de que el ciudadano europeo obtenga compensación administrativa y judicial en caso de vulneración de sus derechos[21]. Respecto a los mecanismos judiciales que tienen los ciudadanos europeos, estos se han podido incorporar al Acuerdo Marco después de llevar a cabo algunas reformas legislativas en el ordenamiento jurídico estadounidense, concretamente, actualizando la Ley federal de arbitraje y adoptando la Ley de recurso judicial[20].

[20]H.R.1428 - Judicial Redress Act of 2015.

[21]Parlamento Europeo, «Working Document on future European Union (EU) - United States of America (US) international agreement on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters», Committee on Civil Liberties, Justice and Home Affairs, PE536.151v02-00, 14 de julio de 2014, pág. 2.

Resumen

Este módulo ha analizado los instrumentos y mecanismos que existen en la normativa actual de protección de datos de la UE para transferir datos personales a terceros Estados. Como se ha podido ver, la regulación existente varía en función de si el tercer Estado en cuestión cumple o no con el nivel adecuado de protección de datos en función de unos parámetros establecidos por la Comisión Europea.

Los casos más problemáticos son aquellos que requieren la transferencia de datos personales por parte de empresas situadas en territorio de la UE a terceros países que no tienen un nivel equivalente de protección de datos. En dichos casos, el RGPD prevé subsanar estas dificultades mediante un previo compromiso de la empresa situada en el tercer Estado de garantizar unas salvaguardas mínimas en el tratamiento de datos personales de ciudadanos europeos. Estos compromisos se regulan mediante la aprobación de cláusulas contractuales tipo, normas corporativas vinculantes, códigos de conducta u otras garantías *ad hoc*. En cualquier caso, el clausulado de estos mecanismos requerirá de previa aprobación por parte de la autoridad de protección de datos del Estado miembro donde está localizada la empresa u organización privada que transfiere los datos.

Un caso especial es que se lleva a cabo para transferir datos entre la Unión Europea y Estados Unidos. Estados Unidos no está en la lista de países que cumplen con un nivel adecuado de protección de datos, según la Comisión Europea, pero a causa de las importantes relaciones comerciales que existen entre la UE y Estados Unidos, fue imperiosa la necesidad de incorporar un sistema especial para regular los flujos de datos personales entre estos dos países.

A día de hoy existen dos mecanismos para transferir datos personales a Estados Unidos: el Escudo de la Privacidad UE-EEUU[22] y el Acuerdo Marco de Protección de Datos entre la UE y Estados Unidos. Tal y como se desprende de este estudio, aunque ambos instrumentos cumplen un propósito de reforzar la protección de datos de los ciudadanos europeos en Estados Unidos incorporando mecanismos de acceso, modificación, eliminación y recurso en territorio estadounidense, es mucha la doctrina que considera que estos instrumentos no son adecuados.

[22]En 2017 va a tener lugar la primera revisión anual de este acuerdo. Ver:https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_06_13_01-ides-idphp.php

Si bien las opiniones en cuanto a la regulación europea existente para transferencias internacionales de datos personales suscita dudas de adecuación, especialmente por lo que respecta a datos transferidos a Estados Unidos, está

claro que tanto el RGPD como el Escudo de la Privacidad UE-EEUU mejoran considerablemente el marco legal anterior compuesto por la DPD y el Acuerdo de Puerto Seguro.

Bibliografía

Bibliografía básica

Blasi Casagran, C. (2017). «Nuevo régimen jurídico para la transferencia de datos entre la UE y los Estados Unidos: ¿Es compatible con la normativa europea de protección de datos?». *Revista General de Derecho Europeo* (núm. 42, págs. 193-217).

González Fuster, G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Londres: Springer.

Guasch Portas, V. (2014). *Las transferencias internacionales de datos en la normativa española y comunitaria*. Madrid: Agencia Estatal Boletín Oficial del Estado.

López Calvo, J. (2017). *Comentarios al Reglamento Europeo de Protección de Datos*. Madrid: Sepin.

Piñar Mañas, J. L. (2016). *Reglamento general de protección de datos. Hacia un nuevo modelos europeo de privacidad*. Madrid: Editorial Reus.

Bibliografía específica

Blasi Casagran, C. (2016). *Global Data Protection in the Field of Law Enforcement. An EU Perspetive*. Routledge / Taylor & Francis Group.

De Busser, E. (2009). *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities*. Antwerpen: Maklu Publishers.

De Hert, P.; Bellanova, R. (2009). *Data protection in the Area of Freedom, Security and Justice. A system still to be fully developed?* (págs. 1-32). European Parliament, Directorate General Internal Policies of the Union, Policy Department C, Citizens' Rights and Constitutional Affairs. PE 410.692.

De Hert, P.; Papakonstantinou, V. (2009). «The PNR Agreement and transatlantic anti-terrorism co-operation: No firm human rights framework on either side of the Atlantic». *Common Market Law Review* (núm. 46, págs. 885-919).

Kokott, J.; Sobotta, C. (2013). «The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR». *International Data Privacy Law* (vol. 3, núm. 4, págs. 222-228).

Omand, D. (2010). *Securing the State (Intelligence and security)*. Oxford: Oxford University Press.

Quesada Gámez, M.; Mincheva, E. (2012). «No data without protection? Re-thinking transatlantic information Exchange for law enforcement purposes after Lisbon». En: P. J. Cardwell (ed.). *EU external relations law and policy in the post-Lisbon era* (págs. 287-312). Berlín: Springer.

Schwartz, P. M. (2014, 22 de julio). «Differing privacy regimes: A mini-poll on mutual EU-US distrust». IAPP.

<https://privacyassociation.org>

Tene, O. (2014, marzo). «The U.S.-EU privacy debate: Conventional wisdom is wrong». *Privacy Perspectives* (núm. 4).

<https://privacyassociation.org>

Tzanou, M. (2017). «European Union Regulation of Transatlantic Data Transfers and Online Surveillance». *Human Rights Law Review* (núm. 0, págs. 1-21).