Internacional

# EL RÉGIMEN JURÍDICO DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES ENTRE EUROPA Y EE. UU.

Leticia López-Lapuente y Mirian Goitia
*Abogadas del Área de Mercantil de Uría Menéndez (Madrid)*

**El régimen jurídico de las transferencias internacionales de datos personales entre Europa y EE. UU.**

*La realización de transferencias internacionales de datos en los últimos años ha supuesto un reto jurídico para las empresas, especialmente en la realización de transferencias de datos de Europa a EE. UU. La falta de seguridad jurídica como consecuencia de las resoluciones emitidas en esta materia han incrementado el riesgo regulatorio inherente a su realización cuando el tercer país al que se transfieren los datos no cuenta con una decisión de adecuación.*

**PALABRAS CLAVE:**
Transferencias internacionales, Decisión de adecuación, Garantías, Seguridad jurídica, Datos personales, Nivel de protección, Unión Europea.

**The legal framework for international transfers of personal data between Europe and the US**

*International transfers of personal data have been challenging for companies in recent years, in particular, from Europe to the US. The lack of legal certainty that decisions on the matter have caused, has increased the regulatory risks inherent to international transfers of data to third countries that have no adequacy decision.*

**KEY WORDS:**
International transfers, adequacy decision, guarantees, legal certainty, personal data, level of protection, European Union.

**FECHA DE RECEPCIÓN: 18-9-2023**

**FECHA DE ACEPTACIÓN: 21-9-2023**

López-Lapuente, Leticia; Goitia, Mirian (2023). El régimen jurídico de las transferencias internacionales de datos personales entre Europa y EE. UU. *Actualidad Jurídica Uría Menéndez*, 63, pp. 234-244 (ISSN: 1578-956X).

# 1. Introducción

Las políticas y regulación que la Unión Europea ha ido desarrollando a lo largo de la última década para regular el derecho a la protección de datos personales ha tenido como resultado que la región europea se sitúe como la que garantiza un nivel de protección de datos más elevado a nivel global. Como resultado, los datos personales de los ciudadanos europeos cuentan con un grado de protección elevado.

La normativa de protección de datos, con su origen en la ya derogada la Directiva 95/46, el Reglamento (UE) 2016/679 general de protección de datos ("RGPD") y las normas nacionales que se han ido dictando (la "Normativa de PD") han establecido un régimen para regular la compartición de datos personales de ciudadanos de la UE con destinatarios que se sitúan en países fuera del EEE y que, al no estar sometidos a las normas europeas en materia de protección de datos, podían no garantizar un nivel de protección de datos adecuado.

La normativa de PD actual —y en particular el RGPD— requiere que, cuando se prevea transferir datos personales a un país tercero —aquel que se encuentre fuera del EEE— o a una organización internacional, los responsables del tratamiento deben asegurar que el tercer país u organización garantiza un nivel de protección de datos adecuado conforme al régimen jurídico de la UE, bien sea porque cuenta con normas similares a las que existen en la UE, o porque el emisor y el destinatario de los datos han acordado que, tras la transferencia internacional de datos, estos datos se tratarán cumpliendo una serie de garantías y cautelas que, como resultado, logren garantizar que esos datos personales son tratados en el tercer país con el mismo grado de protección que en la UE.

A. La decisión de adecuación

Conforme al artículo 45 del RGPD, aquellos países terceros u organizaciones internacionales que garantizan un nivel de protección de datos adecuado pueden ser reconocidos por la Comisión Europea como tales. Para contar con este reconocimiento, la Comisión Europea ha estudiado el nivel de protección de datos que se garantiza en ese tercer país teniendo en cuenta para ello el Estado de Derecho (la legislación en materia de derechos humanos, la seguridad pública, defensa, la legislación penal, el acceso a las autoridades públicas), la existencia y funcionamiento de autoridades de control independientes con responsabilidad de hacer cumplir las normas en materia de protección de datos, los compromisos internacionales asumidos por el tercer país u organización internacional, así como otras obligaciones asumidas de acuerdos o instrumentos jurídicamente vinculantes[1]. Como resultado del análisis del nivel de protección otorgado a los datos personales en el tercer país, en aquellos casos en los que el tercer país u organización internacional garan-

tiza un nivel de protección de datos adecuado, la Comisión Europea los reconoce como países adecuados mediante la emisión de un instrumento legislativo europeo, como es una decisión de adecuación. Algunos de los países que cuentan con una decisión de adecuación son Japón, Argentina, Suiza, Canadá, Andorra, Uruguay, Nueva Zelanda, entre otros[2].

B. Otras garantías y medidas adicionales

En aquellos casos en los que los países terceros no cuentan con una decisión de adecuación, el emisor y el destinatario de los datos deben adoptar las garantías y medidas adicionales que resulten necesarias para alcanzar un nivel de protección equivalente en lo esencial al de la UE en el tratamiento de datos personales. Entre las medidas que propone la Normativa de PD se encuentran las normas corporativas vinculantes, las cláusulas contractuales tipo y códigos de conducta, así como mecanismos de certificación aprobados, todo ello conforme a los artículos 46 y 47 RGPD.

C. Excepciones para situaciones específicas

El artículo 49 del RGPD recoge algunas situaciones específicas en las cuales se pueden llevar a cabo transferencias internacionales de datos a un tercer país o a una organización internacional sin contar con una decisión de adecuación o con garantías y medidas adicionales. Estas excepciones se aplican únicamente a transferencias que son puntuales y no repetitivas, así como cuando afecten únicamente a un número limitado de interesados y cuando resulte necesaria para satisfacer los fines de interés legítimo imperiosos que persigue el responsable del tratamiento y sobre los que no deben prevalecer los intereses o derechos y libertades del interesado.

Las situaciones que dan lugar a que se produzca esta excepción son las que vienen establecidas en el artículo 49 RGPD: que el interesado haya dado su consentimiento para la transferencia propuesta tras haber informado sobre los riesgos asociados; que la transferencia sea necesaria para la ejecución de un contrato o precontrato entre el interesado y el responsable del tratamiento; que la transferencia sea necesaria para la celebración de un contrato en interés del interesado con el responsable del tratamiento y otra persona física o jurídica; que la transferencia sea necesaria por razones importantes de interés público, para la formulación, ejercicio o defensa de reclamaciones o para proteger los intereses vitales del interesado o de otras personas (cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento); y cuando la transferencia se realice desde un registro público en los términos establecidos en los artículos 49.1.g) y 49.2 RGPD.

## 2. Las transferencias internacionales de Europa a EE. UU.

El régimen jurídico aplicable a la realización de transferencias internacionales de datos entre la UE y EE. UU. ha sufrido drásticos cambios y ha sido cuestionado en varias ocasiones en los últimos años. En los próximos epígrafes se van a analizar los distintos instrumentos que se han articulado

para garantizar que las transferencias internacionales de datos entre el EEE y EE. UU. se realizan asegurando un nivel de protección de datos adecuado. Asimismo, se analizarán las causas por las cuales algunos instrumentos han sido considerados insuficientes y, en consecuencia, inválidos, así como la progresión en la sustitución de estos mecanismos por otros, hasta llegar a la aprobación del instrumento que actualmente garantiza la realización de transferencias entre el EEE y EE. UU., el conocido como Marco de Privacidad UE-EE. UU.

Históricamente, EE. UU. ha sido una región donde no se ha garantizado un nivel de privacidad elevado. Los poderes elevados reconocidos en el ámbito de las investigaciones y la seguridad nacional, así como la concepción sobre cómo debe gestionarse el control de los datos por parte del interesado de los datos ha llevado a que los ciudadanos estadounidenses no tengan reconocido un derecho a la protección de datos personales como lo entiende la UE. Por todo ello, EE. UU., por el momento, no ha adoptado normas de privacidad a nivel federal. Sin perjuicio de ello, algunos estados han adoptado normas en materia de privacidad, aunque su ámbito de protección resulta menor que el nivel de protección de datos existente en la UE. Por estas razones, los instrumentos de adecuación que se han pactado con EE. UU. a lo largo de los últimos años no han tenido la ambición de abarcar a toda la región, sino que se han circunscrito únicamente a las empresas que voluntariamente han decidido adherirse a algunos principios en materia de protección de datos.

## 2.1. Puerto seguro

El primer instrumento de adecuación (bajo el artículo 45 RGPD) que reguló la realización de transferencias internacionales entre la UE y EE. UU. fue el *Safe Harbour* (Puerto Seguro) constituido por el Departamento de Comercio de los Estados Unidos el 21 de julio del año 2000. La Comisión Europea emitió la decisión de adecuación mediante la Decisión 2000/520 (la "Decisión" o "Puerto Seguro")[3], por la cual reconocía que este instrumento garantizaba la realización de transferencias internacionales garantizando un nivel de protección adecuado cuando dichas transferencias se realizaban a las entidades que se encontraban adheridas a los principios de Puerto Seguro. Esta Decisión incluye los principios de Puerto Seguro que van dirigidos en exclusiva a las entidades estadounidenses que reciben datos personales de la Unión Europea. Las entidades receptoras de datos personales deben cumplir los requisitos de Puerto Seguro para obtener la correspondiente presunción de "adecuación". En la realización de transferencias internacionales al amparo de este instrumento, el responsable de los datos debía verificar que la empresa destinataria de los datos en EE. UU. estaba incluida en el instrumento Puerto Seguro.

## 2.2. El caso Schrems I

El 25 de junio de 2013, el Sr. Maximilian Schrems presentó una reclamación para que se prohibiera a una red social transferir datos personales a los Estados Unidos. El Sr. Schrems llevaba años siendo usuario de esta red social. Aunque el contrato para el uso del servicio de la red social por parte de ciudadanos europeos se concluía con la filial irlandesa de la red social, los datos personales de los usuarios europeos se transferían a los servidores pertenecientes a la matriz del grupo situados en EE. UU. El Sr. Maximilian Schrems alegaba en su reclamación que se debían prohibir las transferencias de datos a EE. UU. porque el derecho y las prácticas en vigor en EE. UU. no garantizaban un nivel de protección suficiente y equivalente en lo esencial al de la UE[4]. La reclamación del

Sr. Maximilian Schrems llegó a la High Court Irlandesa, que, para resolver sobre el litigio, planteó algunas cuestiones prejudiciales al Tribunal de Justicia de la Unión Europea ("TJUE")[5].

### 2.2.1. SOBRE LAS FACULTADES DE LAS AUTORIDADES NACIONALES DE PROTECCIÓN DE DATOS

El TJUE concluyó que las autoridades nacionales de control, como el Comisionario Irlandés, disponen de una amplia gama de facultades necesarias para garantizar el cumplimiento de sus funciones, entre otras, facultades de investigación, de recabar información y de intervención, como por ejemplo prohibir provisional o definitivamente un tratamiento de datos. Sin embargo, las autoridades de control estatales, en tanto en cuanto deben abarcar los tratamientos de datos realizados en su territorio, no disponen de facultades respecto de los tratamientos de datos que se realizan en un tercer país. Por ello, la autoridad de control nacional es competente en analizar si la transferencia se realizó adoptando las garantías exigidas por la Normativa de PD. No obstante, el TJUE aclaró que, mientras que la decisión de adecuación no haya sido declarada inválida por el TJUE, los Estados miembros (incluyendo las autoridades de control) no pueden adoptar medidas contrarias a la decisión. El TJUE es la única autoridad que puede declarar la invalidez de una decisión adoptada por la Comisión. Por ello, el TJUE analiza la validez de la Decisión.

### 2.2.2. SOBRE LA VALIDEZ DE LA DECISIÓN DE PUERTO SEGURO

El TJUE estableció que el nivel de protección garantizado por un tercer país puede evolucionar y la Comisión Europea debe comprobar periódicamente si el tercer país sigue garantizando un nivel de protección de datos adecuado. En particular, el TJUE establece que esa comprobación es obligatoria cuando hay indicios que generan dudas sobre el nivel de protección ofrecido.

El TJUE reconoció que, si bien la adopción de la presunción de adecuación de las entidades estadounidenses se lograba con la adopción de los principios de Puerto Seguro, la Decisión reconocía la primacía de las exigencias sobre seguridad nacional, interés público y cumplimiento de la ley de EE. UU. sobre los principios de Puerto Seguro. Por ello, las entidades adheridas estaban obligadas a dejar de cumplir los principios de Puerto Seguro si estos resultaban incompatibles con las normas de EE. UU. En este sentido, el TJUE consideró que una norma cuyo objetivo es salvaguardar el derecho a la protección de datos personales de los ciudadanos europeos no puede permitir a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas (en vulneración del derecho fundamental a la vida privada)[6]. Asimismo, no se prevé la posibilidad de que el interesado de los datos ejerza acciones para acceder a los datos personales que le conciernen o para ejercitar el resto de derechos en materia de protección de datos (en vulneración del derecho fundamental a la tutela judicial efectiva)[7]. Adicionalmente, el hecho de que la Decisión no reconozca a EE. UU. como un país que garantiza efectivamente un nivel de protección de datos adecuado vulnera las exigencias del artículo 25.6 de la Directiva 95/46, que requiere que la adopción de una decisión de adecuación exige que se haya constatado que el tercer país garantiza en su legislación interna un nivel de protección de los derechos fundamentales sustancialmente equivalente al garantizado en la UE. En el caso de la Decisión de Puerto Seguro no se cumple este precepto y, por ello, la Decisión resulta inválida.

## 2.3. Privacy Shield

Tras la invalidación de la Decisión en 2014, las transferencias internacionales de datos ente la UE y EE. UU. se realizaban basando estas en otras garantías distintas a la decisión de adecuación hasta que se aprobara la nueva decisión de adecuación 2016/1250 de la Comisión el 12 de julio de 2016 ("Privacy Shield")[8]. El Privacy Shield mantiene un esquema de autocertificación, en virtud del cual, las entidades estadounidenses pueden someterse al cumplimiento de algunos principios complementarios establecidos por el Departamento de Comercio de los Estados Unidos, entre los cuales se encontraban el principio de notificación a los interesados, el principio de integridad de los datos y limitación de la finalidad, el principio de opción a oponerse, el principio de integridad de los datos y limitación de la finalidad, el principio de seguridad, el principio de acceso, el principio de recurso, aplicación y responsabilidad, y el principio de responsabilidad de la transferencia ulterior.

Tras la aprobación del Privacy Shield, las transferencias internacionales de datos entre la UE y EE. UU. se realizaban con seguridad jurídica y con mayor facilidad, lo que ayudaba a agilizar las transacciones entre ambas regiones.

## 2.4. El caso Schrems II

El 16 de julio de 2020, el TJUE se pronunció sobre otra reclamación interpuesta por el Sr. Maximilian Schrems[9] ante las autoridades irlandesas, en particular, la reclamación fue interpuesta contra una red social por realizar transferencias internacionales de datos basadas en la firma de cláusulas contractuales tipo a la matriz de la red social situada en EE. UU. cuando, según el Sr. Maximilian Schrems, este instrumento no garantiza un nivel de protección de datos adecuado en este contexto. Resulta necesario aclarar que la reclamación originaria que da lugar a este litigio se enmarca en el momento temporal en el que, tras la invalidación de la Decisión de Puerto Seguro, aún no se había aprobado el Privacy Shield. No obstante, el TJUE además de analizar el supuesto que dio lugar a la reclamación también se pronunció sobre la validez del Privacy Shield.

### 2.4.1. SOBRE LA REALIZACIÓN DE TRANSFERENCIAS INTERNACIONALES A EE. UU. BASADAS EN SCC

En este sentido, el TJUE concluyó que, en cumplimiento con lo establecido en los artículos 46(1) y 46(2)(c) RGPD, los responsables del tratamiento debían adoptar las garantías adecuadas para garantizar que los interesados de los datos son provistos mediante las SCC de un nivel de protección esencialmente equivalente al que se proporciona en la Unión Europea. En casos en los que el tercer país no haya sido reconocido por la Comisión Europea como un país que garantiza un nivel de protección de datos adecuado, es responsabilidad de los exportadores de los datos adoptar las garantías suficientes, lo cual puede suponer que, además de la adopción de las SCC, se deban adoptar garantías adicionales para asegurar un nivel de protección de datos suficiente. Las SCC son por su naturaleza instrumentos contractuales que garantizan un nivel de protección *inter partes* y no garantizan un nivel adecuado de protección fuera de la relación contractual. En consecuencia, tal y como se estableció en la sentencia Schrems I, las autoridades de protección de datos nacionales deben requerir la suspensión de las transferencias internacionales de datos

si no se están adoptando las garantías necesarias. En este caso, salvo que exista una decisión de adecuación con ese país tercero, en caso de que las SCC resulten una garantía insuficiente, se debe suspender y prohibir la transferencia internacional de datos a EE. UU.

### 2.4.2. SOBRE LA VALIDEZ DEL PRIVACY SHIELD

Finalmente, el TJUE se pronuncia sobre el impacto que tiene en esta reclamación la reciente aprobación del Privacy Shield. En este sentido, el TJUE establece que, aunque la decisión de adecuación del Privacy Shield establece que EE. UU. garantiza un nivel de protección de datos adecuado a los datos transferidos de la UE a organizaciones en los EE. UU. al amparo del Privacy Shield, también establece que, la adherencia a los principios que rigen el instrumento de adhesión puede estar limitada a lo necesario para garantizar la seguridad nacional, el interés público y los requerimientos de cumplimiento. Por lo tanto, estos últimos principios tienen primacía respecto de los principios establecidos en el Privacy Shield.

Por todo lo anterior, el TJUE concluye que la existencia de mecanismos donde ejercitar y obtener la tutela judicial efectiva es inherente al cumplimiento de las normas de la UE y a la existencia de un Estado de Derecho, y que la legislación de un país que no garantiza el ejercicio de este derecho (p. ej., por no facilitar la posibilidad a los interesados de ejercitar sus derechos en materia de protección de datos) no respeta el derecho fundamental a la tutela judicial efectiva y no garantiza un nivel de protección de datos adecuado. En consecuencia, el TJUE invalida el Privay Shield como mecanismo para transferir datos del EEE a EE. UU.

### 2.4.3. EFECTOS DE LA INVALIDACIÓN DEL PRIVACY SHIELD

En este contexto, la organización activista por la privacidad *Non of your business* —en la que participa el Sr. Maximilian Schrems— inició un proceso de reclamaciones en masa (ciento una en total)[10] frente a empresas que realizaban transferencias de datos entre la UE y EE. UU. en las que se alegaba que las transferencias internacionales de datos que se producían por el uso de la integración de dos tipos de *cookies* en las páginas web de los responsables del tratamiento europeos se llevaban a cabo sin garantizar un nivel de protección de datos adecuado. En particular, fueron objeto de estas reclamaciones dos multinacionales tecnológicas. En efecto, varias autoridades de los distintos Estados miembros de la UE emitieron resoluciones sancionadoras que establecían que debía suspenderse la realización de transferencias internacionales de datos del EEE a EE. UU. por no garantizar un nivel de protección de datos adecuado (véanse las resoluciones del CNIL, autoridad italiana, autoridad austríaca, autoridad noruega y autoridad irlandesa), por considerar que la firma de cláusulas contractuales tipo no suponía un instrumento que garantizara un nivel de protección de datos adecuado.

Como resultado de esta sentencia del TJUE, el Comité Europeo de Protección de Datos ("EDPB") adoptó medidas para proporcionar nuevas pautas en la realización de transferencias internacionales de datos. En concreto, el EDPB emitió unas nuevas guías sobre los mecanismos en virtud de los cuales se podrían llevar a cabo transferencias internacionales de datos[11], incorporando la necesidad de que los responsables de los datos llevaran a cabo un estudio del impacto de la transferencia internacional y concluyeran sobre la necesidad o no de adoptar garantías adicionales a

los mecanismos habituales previstos en el RGPD, y proporcionando ejemplos de estas garantías o medidas adicionales, así como los criterios que se debían tomar en consideración para valorar el riesgo de la transferencia y la necesidad de adoptar garantías adicionales. Asimismo, también se actualizaron los modelos de SCC y se publicaron modelos diferenciados para cada tipo de relación (responsable a responsable, responsable a encargado, encargado a responsable y encargado a encargado). Si bien la respuesta por parte del EDPB redujo —en parte— la inseguridad jurídica que se había generado tras la sentencia del TJUE y las resoluciones de las autoridades nacionales, los operadores jurídicos que llevaban a cabo transacciones económicas (y de datos) entre la UE y los EE. UU. se vieron inmersos en un riesgo regulatorio y de inseguridad, ya que la responsabilidad de la adopción de los mecanismos para transferir datos y la justificación de que dichas medidas eran suficientes quedó atribuida a los exportadores de datos.

## 2.5. El actual marco de privacidad entre la UE y EE. UU.

La situación de falta de seguridad jurídica en la realización de transferencias internacionales entre la UE y EE. UU. ha supuesto un obstáculo en la realización de actividades comerciales entre ambas regiones. Además, por la naturaleza de la cuestión, esta situación no podía resolverse con la mera voluntad de los operadores privados, sino que, al tratarse de un tema de seguridad nacional, requería un pacto político entre ambas regiones para facilitar los flujos transfronterizos de datos personales entre la UE y EE. UU.

Tras la invalidación del Privacy Shield, se iniciaron negociaciones políticas entre la UE y EE. UU. para lograr acordar otro instrumento que resultara válido y amparara la realización de transferencias internacionales de datos entre la UE y EE. UU. En octubre de 2022, el presidente Biden emitió una orden ejecutiva[12] en la que se comprometía a adoptar las garantías necesarias para que las actividades de investigación estadounidenses implementaran determinados compromisos de minimización y garantías en materia de protección de datos y, de esta forma, avanzar en la conclusión del acuerdo para la realización de transferencias internacionales de datos entre la UE y EE. UU. acordado entre ambos Gobiernos.

Tras la revisión y adaptación del marco jurídico estadounidense, la Comisión Europea ha vuelto a evaluar el nivel de protección de datos garantizado en EE. UU. y ha considerado que proporciona un nivel de protección de datos adecuado. En consecuencia, la Comisión emitió en julio del año 2023 la decisión de adecuación para la realización de transferencias internacionales de datos desde la UE a EE. UU. (EU-US Data Privacy Framework) (el "Privacy Framework")[13].

El nuevo marco legal sigue un régimen de certificación, en virtud del cual, las empresas estadounidenses deberán adherirse a una serie de principios de protección de datos (p. ej., *principio de limitación de la finalidad, transparencia, tratamiento de categorías especiales de datos, actualización de los datos, minimización y seguridad de los datos*), así como someterse a los poderes de investigación y cumplimiento del Federal Trade Comission y the U.S. Department of Transportation para poder transferir datos personales sin la necesidad de adoptar garantías adicionales. El proceso de certificación deberá renovarse anualmente y las empresas que estaban adheridas al marco legal anterior deberán adherirse al nuevo marco. Aquellas empresas que no se certifiquen y adhieran

al cumplimiento de los principios de protección de datos no se podrán beneficiar del Privacy Framework en la recepción de datos personales enviados desde la UE.

El nuevo Privacy Framework incluye mecanismos vinculantes para regular aquellas materias que el TJUE consideró que no se garantizaban y, en consecuencia, considerar que las entidades estadounidenses adheridas no proporcionaban un nivel de protección de datos adecuado. En particular, el Privacy Framework limita el acceso a los datos de ciudadanos europeos a los servicios de inteligencia estadounidenses al someterlo al cumplimiento de determinados principios de necesidad y proporcionalidad. Asimismo, se establece un órgano jurisdiccional al que los ciudadanos de la UE pueden acceder (Data Protection Review Court). Entre otras funciones, este órgano podrá ordenar la supresión de los datos personales en el caso de que se hayan obtenido de forma contraria a lo establecido en el Privacy Framework (p. ej., en vulneración de alguno de los principios) o analizar si las agencias de inteligencia estadounidenses recaban y tratan los datos personales de forma válida. Para ello, este órgano jurisdiccional podrá adoptar decisiones vinculantes.

Asimismo, las entidades adheridas deberán cumplir con la obligación de permitir el acceso gubernamental a los datos que tienen estas entidades. Para que las entidades estadounidenses puedan adherirse al Privacy Framework, deberán cumplir con las nuevas obligaciones en materia de protección de datos que se establecen, entre otros, suprimir los datos cuando no resulten necesarios para la finalidad para la que fueron recabados y garantizar la continuidad de la protección de los datos cuando se comunican a terceros.

De conformidad con lo establecido en el Privacy Framework, este instrumento estará sujeto a revisiones periódicas. La primera de ellas se llevará a cabo al año desde su entrada en vigor, cuando se verificará que todos los elementos incorporados en el Privacy Framework han sido debidamente implementados en el ordenamiento jurídico estadounidense y funcionan de forma efectiva.

Sin perjuicio de lo anterior, desde la publicación del Privacy Framework ya se ha anunciado la interposición de recursos contra la validez de este acuerdo por parte de activistas y de personas físicas. Por ello, habrá que seguir de cerca los pronunciamientos en esta materia que vayan emitiendo los órganos y tribunales de cada Estado miembro.

# 3. Conclusiones

La realización de transferencias internacionales de datos que garanticen un nivel de protección adecuado ha resultado un reto jurídico en los últimos años. Actualmente, el régimen de trasferencias internacionales a EE. UU. queda amparado, por el momento, en el Privacy Framework cuando el destinatario de los datos esté adherido a este instrumento. Además, el acuerdo político entre la UE y EE. UU. se está reforzando con el trabajo de organizaciones internacionales cuyo objetivo es elevar este consenso a los flujos transfronterizos que se llevan a cabo a nivel global. En consecuencia, el Privacy Framework, además de ser un acuerdo bilateral entre la UE y EE. UU., podría generar un impacto y adoptarse como estándar para garantizar que el intercambio transfronterizo de datos a nivel global se realiza también al amparo de estos principios.

Sin perjuicio de lo anterior, tras las sentencias del TJUE en los casos Schrems I y Schrems II, las resoluciones sancionadoras de algunas autoridades de control europeas de protección de datos, y la publicación de las nuevas guías sobe garantías para la realización de transferencias internacionales emitidas por el CEPD, los exportadores de datos sufren aún las consecuencias de la inseguridad jurídica y asumen cierto riesgo regulatorio a la hora de realizar transferencias internacionales.

Lo anterior se debe a que la fórmula de medidas que se debe adoptar para garantizar que una transferencia se realiza garantizando un nivel de protección de datos adecuado depende de las circunstancias particulares de cada caso, y en aquellos casos en los que no se transfieren datos en virtud de una decisión de adecuación, sino mediante otros mecanismos, como pude ser la firma de las SCC, el exportador de datos debe elegir y demostrar qué medidas resultan suficientes como para garantizar que las transferencias internacionales se realizan asegurando un nivel de protección de datos adecuado. Además, la complejidad y riesgos asociados a esta cuestión no solo se aplica a la realización de transferencias internacionales a EE. UU., sino también a la realización de transferencias internacionales de datos a cualquier tercer país u organización internacional que no cuente con una decisión de adecuación.

## Notas

1 Artículo 45 RGPD.

2 El listado de países adecuados que cuentan con una decisión de adecuación se puede consultar en este enlace: https://www.aepd.es/preguntas-frecuentes/6-transferencias-internacionales-bcr-codigos-de-conducta/1-transferencias-internacionales/FAQ-0605-que-paises-se-consideran-con-un-nivel-adecuado-a-efectos-del-articulo-45-del-rgpd.

3 Decisión 2000/520 de la Comisión Europea: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32000D0520.

4 El motivo principal del argumento suscitado por el Sr. Maximilian Schrems se basa en que las agencias estadounidenses, como el National Security Agency (NSA), y otros organismos federales, como el Federal Bureau of Investigation (FBI), pueden acceder a los datos personales en el contexto de ejercitar sus deberes de vigilancia, llevando a cabo en ocasiones interceptaciones a gran escala.

5 STJUE 6 de octubre de 2015, Caso C-362/14: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362.

6 Garantizado en el artículo 7 de la Carta Europea de Derechos Fundamentales (la "**Carta**").

7 Garantizado en el artículo 47 de la Carta.

8 Decisión de ejecución (UE) 2016/1250 de la Comisión, sobre la adecuación de protección conferida por el Escudo de Privacidad UE-EEUU (Privacy Shield): https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D1250&from=es.

9 STJUE Caso C-311/18, de 16 julio de 2020: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311.

10 NOYB. EU-US Transfers Complaint Overview: https://noyb.eu/en/eu-us-transfers-complaint-overview.

11 Guías sobre mecanismos para la realización de transferencias internacionales de datos del CEPD (link).

12 Orden ejecutiva para la implementación del EU-US Data Privacy Framework (link).

13 Decisión de adecuación UE-EEUU (Data Privacy Framework) (link).