FACULTAD DE DERECHO

LAS TRANSFERENCIAS INTERNACIONALES DE DATOS ENTRE LA UNIÓN EUROPEA Y ESTADOS UNIDOS TRAS LA INVALIDEZ DEL ESCUDO DE PRIVACIDAD

Autora: Claudia Posse Acha
5º, E-5
Derecho Internacional Privado

Tutor: Diego Agulló Agulló

Madrid
Abril 2022

RESUMEN:

La transferencia de datos personales entre la UE y EEUU es la mayor en volumen del mundo y supone un gran interés económico para ambas potencias. Por ello, a lo largo de los últimos años, se han desarrollado diferentes instrumentos jurídicos para facilitar dicha transferencia, entre los que destaca el Acuerdo del Puerto Seguro y el Acuerdo del Escudo de Privacidad. No obstante, dadas las discrepancias en la percepción de la protección de datos personales entre la UE y EEUU, la jurisprudencia del Tribunal de Justicia de la UE, en sus Sentencias Schrems I y Schrems II, ha invalidado sendos acuerdos por considerar que no cumplen con los estándares de protección exigidos por la Unión. Ante la falta de un acuerdo, los operadores de ambos lados del Atlántico han de manejar mecanismos alternativos de transferencia de datos personales que da lugar a una situación de confusión.

PALABRAS CLAVE:

Escudo de Privacidad, Puerto Seguro, transferencias internacionales de datos personales, Schrems I, Schrems II, Directiva 95/46/CE, Reglamento General de Protección de Datos.

ABSTRACT:

The transfer of personal data between the EU and the US, the largest in volume in the world, is of great economic interest to both powers. Therefore, over the last few years, different legal instruments have been developed to facilitate this transfer, among which the Safe Harbour Agreement and the Privacy Shield Agreement stand out. However, given the discrepancies in the perception of personal data protection between the EU and the US, the EU Court of Justice, in Schrems I and Schrems II, has invalidated the two agreements on the grounds that they do not comply with the standards of protection required by the Union. In the absence of an agreement, operators on both sides of the Atlantic must manage alternative mechanisms for the transfer of personal data, which leads to confusion.

KEY WORDS:

Privacy Shield, Safe Harbour, international data transfers, Schrems I, Schrems II, Directive 95/46/CE, General Data Protection Regulation.

ÍNDICE

LISTADO DE ABREVIATURAS

EEUU: Estados Unidos.

CDFUE: Carta de Derechos Fundamentales de la UE.

CEPD: Comité Europeo de Protección de Datos.

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

TFUE: Tratado de Funcionamiento de la Unión Europea.

TJUE: Tribunal de Justicia de la Unión Europea.

UE: Unión Europea.

I. INTRODUCCIÓN

1. OBJETO

Tras la proliferación y rápido desarrollo de la tecnología a finales del siglo pasado, el mundo del Derecho ha venido tratando de regular este nuevo fenómeno. Sin duda, uno de los desafíos más importantes impuestos por el avance de la tecnología es la regulación de los datos personales de sus usuarios. La recogida e intercambio de dichos datos ha ido aumentando de manera exponencial en los últimos años, permitiendo su acceso en una escala sin precedentes tanto al sector privado como al público.[1] Además, dado que vivimos en un mundo globalizado en el que las economías de los países están interrelacionadas, surge un reto añadido: las transferencias internacionales de datos, fundamentales para la expansión del comercio y la cooperación internacionales.[2]

Este trabajo se centrará, en concreto, en las transferencias internacionales de datos entre la UE y EEUU. En especial, tras la reciente invalidez del Escudo de Privacidad. El estudio de esta relación es de vital importancia, ya que la transferencia de datos entre ambas potencias es la mayor en volumen de todo el mundo. Además, la UE y EEUU comparten una extensa y altamente integrada relación comercial y de inversión, en la cual el tráfico de servicios de la tecnología de la información y las comunicaciones está valorado en más de 264.000 millones de dólares (Congressional Research Service, 2021, p. 5).

2. ESTRUCTURA

Por lo tanto, es conveniente analizar esta relación basada en la transferencia internacional de datos tanto por su volumen como por su relevancia económica. Para ello, este trabajo analizará el primer Acuerdo entre la UE y EEUU en materia de

[1] Considerando 6 del RGPD.
[2] Considerando 101 del RGPD.

protección de datos, el Puerto Seguro, seguidamente de la sentencia del TJUE que causó su invalidación. A continuación, se estudiará el segundo Acuerdo aprobado por las dos potencias, el Escudo de Privacidad, para también examinar la sentencia que lo declaró inválido. Finalmente, se reflexionará acerca del escenario de las transferencias internacionales de datos entre la UE y EEUU tras la invalidez del Escudo de Privacidad, proponiendo alternativas tanto a corto como a largo plazo.

No obstante, antes de comenzar a analizar jurídicamente las transferencias internacionales de datos entre la UE y EEUU, es oportuno adelantar que cada potencia tiene una aproximación notablemente diferente al entendimiento de los datos personales, lo cual influenciará directamente el objeto de estudio de este trabajo.

La primera gran diferencia estriba en el hecho de que en la UE la privacidad y el derecho a la protección de datos de carácter personal son derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE). Asimismo, el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) establece que 'toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan'. Sin embargo, ni la Constitución Federal de EEUU de 1787 ni sus posteriores enmiendas reconocen expresamente ninguno de estos derechos (Álvarez Caro y Recio Gayo, 2015, p. 3). En su lugar, EEUU entiende la privacidad como un producto objeto de comercialización (Schwartz y Peifer, 2017, p. 121). Por lo tanto, sus leyes la consideran un derecho a la protección del consumidor en el mercado de la información, pero no un derecho fundamental ligado a la dignidad de la persona (Schwartz y Peifer, 2017, p. 132).

La segunda gran diferencia entre el planteamiento de la protección de los datos personales en las dos potencias se trata de que, mientras la UE ofrece una legislación sumamente detallada y aplicable a todos los sectores a través de un sistema *top-down*, EEUU carece de este marco normativo consolidado y presenta en su lugar un planteamiento sectorial y descentralizado caracterizado por una mezcla de legislación, reglamentación y autorregulación (Álvarez Caro y Recio Gayo, 2015, p. 3).

Por último, la tercera gran diferencia en la aproximación a la protección de datos personales es que la UE ofrece, a través de las figuras del Responsable y del Encargado del tratamiento de datos y de las autoridades nacionales de control, una vía directa y fácil para la reclamación de infracciones. Sin embargo, EEUU adolece de la falta de este

mecanismo y plantea como alternativa la consideración de la Comisión Federal del Comercio como cuerpo regulatorio responsable de la protección de datos personales, aunque su principal razón de ser es la protección de los derechos de los consumidores (Maldonado, 2020, p. 16).

Estas claras diferencias que presentan la UE y EEUU en el entendimiento de los datos personales pueden ser fácilmente justificadas teniendo en cuenta el pasado de ambas partes. Por un lado, como consecuencia de la experiencia de Europa con regímenes fascistas y totalitarios en los cuales las autoridades se inmergían en la vida privada de sus ciudadanos, hoy en día los europeos exigen estrictas medidas de protección de datos personales (Congressional Research Service, 2021, p. 2). En contraposición, en EEUU, por la vivencia de históricos ataques terroristas, sus ciudadanos permiten la vigilancia y supervisión de información sensible por parte de las autoridades con la pretensión de garantizar la seguridad nacional (Maldonado, 2020, p. 20).

3. METODOLOGÍA

El presente trabajo se ha llevado a cabo a través de una revisión cronológica de fuentes de información primarias consistentes en los mecanismos jurídicos que han ido regulado las transferencias internacionales de datos entre la UE y EEUU. Además, este marco teórico se ha llevado a la práctica a través de, por un lado, una investigación del escenario jurídico actual tras la invalidez del Escudo de Privacidad y, por otro lado, una exploración de la jurisprudencia más destacable al respecto, en concreto, del TJUE.

Esta indagación no persigue ofrecer un mero estudio de la evolución de las transferencias internacionales de datos trasatlánticas, sino también proponer diferentes alternativas ante la presente falta de un tercer acuerdo. Para ello, se han revisado fuentes secundarias recabadas de autores tanto nacionales como internacionales. Esta investigación de la doctrina más relevante ha permitido identificar y justificar las posturas de apoyo o rechazo hacia los diferentes esfuerzos normativos propuestos para proteger los datos personales que viajan de un lado al otro del Atlántico.

II. DEL PUERTO SEGURO A SCHREMS I

1. CONTEXTO NORMATIVO

Consciente de la importancia de los flujos de datos personales en la actual sociedad de la información, la legislación de la UE ha proporcionado desde sus orígenes una serie de mecanismos que permiten las transferencias internacionales de datos de la UE a terceros países u organizaciones garantizando en ellos el mismo nivel de protección europeo (Comisión Europea, 2017, p. 4). Entre las normas que los regulan, destacan el Reglamento General de Protección de Datos (UE) 2016/679 (en adelante, RGPD), por ser el actual régimen jurídico vigente, y la derogada Directiva 95/46/CE[3], por ser ésta la base legal en la que se basaron los dos Acuerdos confeccionados para la transferencia internacional de datos entre la UE y EEUU.

1.1. Definición de transferencia internacional de datos personales

Cabe destacar que ni la Directiva 95/46/CE ni el RGPD definen el concepto de transferencia internacional de datos personales. A efectos del RGPD, las transmisiones de datos personales que se producen entre los Estados Miembros de la UE no tienen la consideración de transferencia internacional (artículo 4.23 RGPD). Por exclusión, las transferencias internacionales de datos personales suponen un tratamiento de datos personales en el que confluyen, al menos, un Estado comunitario y un tercer país u organización internacional situado fuera de la UE (Rodríguez Ayuso, 2021, p. 344).

Son dos sus elementos caracterizadores. El primero de ellos es que se trate de un tratamiento de datos personales, es decir, que afecte a una persona física identificada o identificable, siempre y cuando dicho sujeto esté dentro del ámbito de aplicación material y territorial del RGPD. En segundo lugar, el tratamiento debe tener la consideración de transferencia internacional. En este sentido, el TJUE, en el caso

[3] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO 1995 L 281.

Lindqvist[4], ha contribuido a delimitar el contenido de esta figura al interpretar que la difusión de datos personales en una web desde un Estado Miembro no implica una transferencia de datos pese a ser accesibles desde un tercer país. Sin embargo, los servicios de computación en la nube sí se consideran transferencias internacionales, ya que implican un tratamiento de datos que requieren el envío de información a proveedores que, en su caso, se encuentran en terceros países (Piñar Mañas, 2016, pp. 432-433).

1.2. Las transferencias internacionales de datos en la Directiva 95/46/CE

En el ámbito de la UE, la protección de datos se reguló por primera vez en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos. Este instrumento jurídico vino a armonizar las normativas nacionales sobre la materia con el fin de garantizar un elevado nivel de protección y la libre circulación de datos personales entre los diferentes Estados Miembros (Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2018, p. 33).

La Directiva regulaba en su Capítulo IV las transferencias internacionales de datos, estableciendo con carácter general que éstas sólo eran posibles cuando el tercer país en cuestión 'garantice un nivel de protección adecuado' (artículo 25.1). En caso contrario, la transferencia estaba prohibida salvo que se diese alguna de las excepciones que enumeraba el artículo 26, entre las que se encontraba que el Responsable del tratamiento ofreciese garantías suficientes de los derechos de los interesados.[5] Conforme al artículo 25.6, la Comisión podía hacer constar que un país tercero garantizaba un nivel de protección adecuado a la vista de su legislación interna o de sus compromisos internacionales a efectos de protección de la vida privada, de las libertades o de los derechos fundamentales de las personas.

[4] STJUE (Gran Sala), de 6 de noviembre de 2003, asunto C-101/01, Göta hovrät (Suecia) c. Lindqvist, apartado 71.
[5] Ver Cordero Álvarez, 2019, p. 68.

1.3. Las transferencias internacionales de datos en el RGPD

Como adelantábamos, la Directiva 95/46/CE fue derogada y sustituida por el vigente RGPD. Ello fue en parte por los rápidos avances de la tecnología, los cuales requerían una normativa actualizada, y en parte con el objeto de acabar con las diferencias de interpretación y aplicación de la Directiva entre los Estados Miembros.

El RGPD regula las transferencias de datos personales a terceros países u organizaciones internacionales en su Capítulo V, estableciendo un régimen basado en tres supuestos (Piñar Mañas, 2016, p. 432). El primero de ellos se basa en una decisión de adecuación de la Comisión (artículo 45), el cual se mantiene como el principal presupuesto legal jurídicamente habilitante al permitir una mayor libertad de flujo internacional de datos personales (Gonzalo Domenech, 2019, p. 271). El segundo supuesto se basa en la prestación de garantías adecuadas (artículo 46), entre las que se encuentran las normas corporativas vinculantes (artículo 47). Finalmente, el tercer supuesto se basa en las excepciones previstas en el artículo 49. A continuación, se analizará cada uno de estos mecanismos.

1.3.1. Transferencias basadas en una decisión de adecuación

El RGPD establece que, para realizar una transferencia de datos personales a un tercer país u organización internacional, será necesaria una decisión de adecuación de la Comisión Europea que establezca que ese tercer país u organización internacional garantiza un nivel de protección adecuado. De existir dicha decisión de la Comisión Europea, el exportador de datos personales a un tercer país u organización internacional prescindiría de la obligación de obtener una autorización previa o de aportar garantías adicionales (Comisión Europea, 2017, p. 4).

La evaluación de la Comisión Europea se elaborará sobre los elementos que enumera el artículo 45.2 RGPD y teniendo en cuenta el Considerando 104 del RGPD. Siguiendo la categorización propuesta por Piñar Mañas (2016, p. 442), estos elementos a considerar pueden clasificarse en tres grupos:

1) El marco jurídico general en sentido amplio. Es decir, la existencia de un Estado de Derecho, el respeto de los derechos y libertades fundamentales, la legislación y jurisprudencia disponible, el reconocimiento de derechos, el acceso de las autoridades públicas a los datos personales y la necesidad de garantizar las transferencias ulteriores de datos.
2) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país. Éstas deben de cooperar con las autoridades de la UE y de los Estados Miembros.
3) Los compromisos internacionales asumidos. En particular, en materia de protección de datos.

Tras esta evaluación, la Comisión Europea podrá adoptar un acto de ejecución declarando el nivel de protección adecuado de un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional (artículo 45.3 RGPD) que tendrá eficacia directa en todos los Estados Miembros (Polo Roca, 2021, p. 339). El acto de ejecución especificará su ámbito de aplicación territorial y sectorial y, en su caso, determinará la autoridad o autoridades de control. Además, deberá establecer un mecanismo de revisión de una periodicidad de, al menos, cuatro años que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional (artículo 45.3 RGPD).

La decisión de adecuación adoptada podrá ser posteriormente derogada, modificada o suspendida mediante otro acto de ejecución de la Comisión Europea, en la medida necesaria y sin efecto retroactivo, si la información disponible sobre el tercer país u organización internacional en cuestión revela que este último ya no garantiza un nivel de protección adecuado (artículo 45.5 RGPD).

1.3.2. Transferencias basadas en garantías adecuadas

A falta de una decisión de adecuación, ‘el Responsable o el Encargado del tratamiento sólo podrá transmitir datos personales a un tercer país u organización

internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas' (artículo 46.1 RGPD).

Es preciso señalar que el RGPD distingue entre garantías adecuadas que no requieren autorización previa y las que sí. El artículo 46.2 dispone que las garantías adecuadas podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por medio de un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; por medio de normas corporativas vinculantes del artículo 47; por cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control y aprobadas por la Comisión; mediante un código de conducta[6] o, finalmente, mediante un mecanismo de certificación.[7]

Por su parte, el artículo 46.3 establece que siempre que exista autorización de la autoridad de control competente, las garantías adecuadas podrán igualmente ser aportadas, en particular, mediante cláusulas contractuales entre el Responsable o el Encargado y el Responsable, Encargado o destinatario de los datos personales en el tercer país u organización internacional o, en segundo lugar, mediante disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

De este modo, el RGPD refuerza las transferencias internacionales por medio de la introducción de esta nueva vía. A diferencia de la Directiva 95/46/CE, que consideraba la prestación de garantías adecuadas como una excepción a la regla general, el RGPD las añade como supuesto admisible de legitimación de las transferencias junto con las decisiones de adecuación (Rodríguez Ayuso, 2021, p. 351). Además, el RGPD introduce nuevos instrumentos de transferencia internacional, como son los códigos de conducta y los mecanismos de certificación[8], con el fin de 'aportar soluciones mejor adaptadas a las exigencias de las transferencias internacionales, que reflejen, por ejemplo, las características y necesidades específicas de un determinado ámbito o sector industrial, o de flujos de datos concretos' (Comisión Europea, 2017, p. 4).

[6] Junto con compromisos vinculantes y exigibles del Responsable o el Encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.
[7] Junto con compromisos vinculantes y exigibles en los mismos términos que los códigos de conducta.
[8] Por ejemplo, sellos y marcas de privacidad.

1.3.3. Excepciones para situaciones específicas

Finalmente, en ausencia de los dos mecanismos anteriores, es decir, de una decisión de adecuación o de garantías adecuadas, el RGPD permite realizar una transferencia de datos personales a un tercer país u organización internacional únicamente si se cumple alguna de las condiciones previstas en los apartados a) a g) del artículo 49 RGPD. Éstas incluyen la prestación del consentimiento explícito, la celebración o ejecución de un contrato y razones de interés público.

Por último, el mismo artículo recoge una excepción más, con objeto de dar la mayor cobertura posible a las transferencias internacionales (Polo Roca, 2021, p. 356). Incluso si no se da alguna de las excepciones recogidas en los apartados mencionados en el párrafo anterior, la transferencia se podrá llevar a cabo si no es repetitiva, afecta sólo a un número limitado de interesados y es necesaria a los fines de intereses legítimos imperiosos perseguidos por el Responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado. El Responsable del tratamiento tendrá que evaluar todas las circunstancias concurrentes en la transferencia de datos y ofrecer garantías apropiadas en lo concerniente a la protección de datos personales. Además, el Responsable del tratamiento informará a la autoridad de control y al interesado de la transferencia y a este último, de los intereses legítimos imperiosos perseguidos (artículo 49 RGPD).

2. EL PUERTO SEGURO Y SU INVALIDACIÓN

2.1. El Puerto Seguro

Con la llegada de la Directiva 95/46/CE en la UE y ante la falta de una legislación comprehensiva sobre la protección de datos en EEUU, las empresas y organizaciones americanas temieron una limitación de su capacidad de actuación al otro lado del Atlántico (Álvarez Caro y Recio Gayo, 2015, p. 3). Por ello, en 1998, el Departamento de Comercio de EEUU y la Comisión Europea comenzaron negociaciones para diseñar un mecanismo que facilitase a los operadores americanos

garantizar el 'nivel de protección adecuado' exigido por la Directiva 95/46/CE. Fue así cómo, dos años más tarde, se alcanzó el primer Acuerdo entre EEUU y la UE para permitir la transferencia transatlántica de datos personales, conocido como el Puerto Seguro. Este pacto se plasmó en la Decisión de la CE, 2000/520/CE, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios del Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

El instrumento utilizado se basaba en un sistema de autocertificación en el que las entidades estadounidenses adheridas se comprometían a gestionar los datos personales de los ciudadanos europeos conforme a los principios suscritos en el Acuerdo y administrados por el Departamento de Comercio de Estados Unidos.[9] Cabe destacar que el Puerto Seguro en su Anexo I, recogía una serie de limitaciones a estos principios, entre las que se encontraban las exigencias derivadas de la seguridad nacional, el interés público y el cumplimiento de la ley. Una vez que las empresas se adherían voluntariamente a dichos principios, se presumía que cumplían con el nivel de protección adecuado exigido por la Directiva 95/46/CE (Uría Gavilán, 2016, p. 265).

No obstante, el Acuerdo del Puerto Seguro se convirtió en objeto de duras críticas cuando en 2013 un exempleado de la Agencia de Seguridad Nacional americana, Edward Joseph Snowden, hizo públicas una serie de operaciones de vigilancia masiva e indiscriminada llevadas a cabo por el gobierno estadounidense que ponían de manifiesto las deficiencias del Acuerdo (Castellanos Rodríguez, 2017, p. 17).

A raíz de estos hechos, la Comisión emitió dos comunicaciones en las que advertía de los retos y riesgos derivados de la revelación de la existencia de programas estadounidenses de recopilación de información de inteligencia y consideró que el fundamento del régimen del Puerto Seguro debía reforzarse. En estas comunicaciones, la Comisión formuló trece Recomendaciones para una revisión del Acuerdo y, en consonancia con éstas, se iniciaron conversaciones con las autoridades estadounidenses a fin de abordar el refuerzo del régimen del Puerto Seguro. En este contexto, el 6 de octubre de 2015, el TJUE publicó la Sentencia Data Protection Commissioner contra

[9] En concreto, los principios de notificación, opción, transferencia ulterior, seguridad, integridad de los datos, acceso y aplicación.

Facebook Ireland Ltd y Maximillian Schrems, conocida como Schrems I, por la que ulteriormente se declaró inválida la Decisión 200/520/CE.

2.2. La invalidación del Puerto Seguro. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015 (Asunto C-362/14): Schrems I.

Basándose en las declaraciones de Edward Joseph Snowden, en junio de 2013, el Sr. Maximillian Schrems, usuario de Facebook, presentó ante la autoridad irlandesa de protección de datos una reclamación en virtud de la cual solicitaba que se suspendiera la transferencia de sus datos personales efectuada por Facebook Ireland a su matriz Facebook Inc., establecida en los Estados Unidos, donde eran objeto de tratamiento. El Sr. Schrems alegó que el Derecho y las prácticas en vigor en EEUU no garantizaban una protección suficiente de los datos personales conservados en su territorio contra las actividades de vigilancia practicadas por las autoridades públicas. Dicha reclamación fue desestimada por la autoridad de control de Irlanda, pues consideró que no estaba obligada a investigar sobre los hechos. Además, añadió que EEUU ofrecía un nivel adecuado de protección como ya había sido declarado anteriormente por la Comisión Europea en la Decisión 2000/520/CE.[10]

Frente a la decisión de la autoridad de control, el Sr. Schrems interpuso un recurso ante el Tribunal Superior de Irlanda, el cual consideró que la *quaestio litis* debía apreciarse a la luz del Derecho de la Unión.[11] En esas circunstancias, el Tribunal Superior decidió suspender el procedimiento y plantear al TJUE dos cuestiones prejudiciales preguntando *'en sustancia si, y en qué medida, el artículo 25.6 de la Directiva 95/46/CE, entendido a la luz de los artículo 7, 8 y 47 de la Carta, debe interpretarse en el sentido de que una decisión, como la Decisión 2000/520/CE (...) impide que una autoridad de control*'- en este caso la de Irlanda- '*pueda examinar la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de datos personales que la conciernen*', cuando éstos se hayan transferido a

[10] Apartados 26-30 de Schrems I.
[11] Apartado 34 de Schrems I.

un tercer país- en este caso EEUU- cuando esa persona alegue que dicho Estado no garantiza un nivel de protección adecuado.[12]

El TJUE resolvió sobre las facultades de las autoridades de control, pero también se pronunció, como analizaremos a continuación, sobre la validez del Puerto Seguro. El TJUE justifica esta decisión en las dudas que el Tribunal Superior comparte con el Sr. Schrems sobre el nivel de protección adecuado de EEUU en el sentido del artículo 25 de la Directiva 95/46/CE, lo que conduce a reflexionar sobre la validez del Acuerdo.[13]

2.2.1. Sobre las facultades de las autoridades nacionales de control ante una decisión de adecuación

Respecto esta cuestión, el TJUE estima que la existencia de una decisión de adecuación de la Comisión que declara que un tercer país garantiza un nivel de protección adecuado no puede dejar sin efecto ni limitar las facultades expresamente reconocidas a las autoridades nacionales de control en la Directiva 95/46/CE. [14] Entre éstas se encuentra la competencia para comprobar si una transferencia de datos personales desde el Estado Miembro de esa autoridad hacia un tercer país respeta las exigencias establecidas por la Directiva.[15]

El TJUE recuerda que es este tribunal el único órgano competente para declarar la invalidez de un acto normativo de la Unión, como lo es una decisión de adecuación de la Comisión.[16] Así, mientras que el TJUE no declare tal invalidez, las autoridades de control independientes no pueden adoptar medidas contrarias a esa decisión dado que ésta tiene carácter obligatorio para todos los Estados Miembros destinatarios y vincula por tanto a todos sus órganos.[17] No obstante, el TJUE matiza esta cuestión añadiendo que aunque las autoridades de control no pueden declarar inválida una decisión como la

[12] Apartados 36-37 de Schrems I.
[13] Apartado 67 de Schrems I.
[14] Apartado 53 de Schrems I.
[15] Apartado 47 de Schrems I.
[16] Apartado 61 de Schrems I.
[17] Apartados 51-52 de Schrems I.

2000/520/CE, sí son competentes para examinar una reclamación como la interpuesta por el Sr. Schrems.[18]

Concretamente, el TJUE contempla las dos posibilidades que pueden surgir ante una solicitud como la planteada en este caso y determina cómo debe actuar la autoridad de control nacional. Por un lado, en el supuesto de que ésta '*llegue a la conclusión de que los datos alegados en apoyo de esa solicitud son infundados y la desestime por ello, la persona que haya presentado la solicitud debe disponer de recursos jurisdiccionales que le permitan impugnar esa decisión lesiva para ella ante los tribunales nacionales (…) esos tribunales están obligados a suspender el procedimiento y plantear al TJUE una cuestión prejudicial de validez si estiman que uno o varios de los motivos de invalidez alegados por las partes o, en su caso, suscitados de oficio son fundados*'.[19] Por otro lado, cuando esa autoridad considere fundadas las alegaciones expuestas, debe tener capacidad para comparecer en juicio ante los tribunales nacionales 'para que éstos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al TJUE una cuestión prejudicial sobre la validez de ésta'.[20]

2.2.2. Sobre la validez del Puerto Seguro

A continuación, el TJUE procede a examinar la validez de la Decisión 2000/520/CE. Su análisis comienza en el artículo 1 de la Decisión, en el que la Comisión manifestó que los principios del Puerto Seguro garantizan un nivel adecuado de protección de datos personales transferidos desde la UE a entidades establecidas en EEUU.[21] El TJUE afirma que un sistema de autocertificación como el previsto en esta Decisión no es por sí mismo contrario a la exigencia del artículo 25.6 de la Directiva 95/46/CE. No obstante, precisa que la fiabilidad de un sistema de estas características descansa '*en el establecimiento de mecanismos eficaces de detección y de control que permitan identificar y sancionar en la práctica las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales, en especial del derecho al*

[18] Apartado 63 de Schrems I.
[19] Apartado 64 de Schrems I.
[20] Apartado 65 de Schrems I.
[21] Apartado 79 de Schrems I.

respeto de la vida privada y del derecho a la protección de los datos personales'.[22] Sobre la base de los fundamentos jurídicos que se exponen a continuación, el TJUE entendió que el Puerto Seguro no cumplía con este requisito de fiabilidad, lo cual supuso su invalidez.

En primer lugar, el TJUE advirtió de que los principios del Puerto Seguro sólo se aplican a las entidades autocertificadas voluntariamente. Por lo tanto, no se exige que las autoridades públicas estadounidenses se sometan a los mismos.[23] Además, el Acuerdo no contiene constataciones suficientes sobre las medidas con las que EEUU garantiza un nivel de protección adecuado.[24]

En segundo lugar, el TJUE señala que el Acuerdo 'reconoce la primacía de las exigencias de seguridad nacional, interés público y cumplimiento de la ley de EEUU sobre los principios del Puerto Seguro' por lo que 'las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión están obligadas sin limitación a dejar de aplicar esos principios cuando éstos entren en conflicto con esas exigencias'.[25] El TJUE apreció que esta situación suponía una injerencia de las autoridades estadounidenses 'en los derechos fundamentales de las personas cuyos datos personales se transfieren o pudieran transferirse desde la UE a EEUU'.[26] Además, el tribunal alegó que la Decisión 2000/520/CE no contiene ninguna constatación sobre la existencia en EEUU de reglas estatales destinadas a limitar dichas injerencias.[27] En consecuencia, el TJUE considera que '*una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta'*.[28]

[22] Apartado 81 de Schrems I.
[23] Apartado 82 de Schrems I.
[24] Apartado 83 de Schrems I.
[25] Apartado 86 de Schrems I.
[26] Apartado 87 de Schrems I.
[27] Apartado 88 de Schrems I.
[28] Apartado 94 de Schrems I. Ver Uría Gavilán, E. (2016). 'Derechos fundamentales *versus* vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 *Schrems*'. *Revista de Derecho Comunitario Europeo*, 53, pp. 270-271; y Puerto, M.I. y Sferrazza, P. (2017). La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional. *Revista Derecho del Estado*. 40 (dic. 2017), pp. 225-228.

En tercer lugar, el Tribunal señala que el Puerto Seguro no pone de manifiesto la existencia de una protección jurídica eficaz contra las citadas injerencias[29] y destaca que '*una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta'*.[30]

Por último, la sentencia Schrems I destaca que el artículo 3.1 del Puerto Seguro priva a las autoridades nacionales de control de las facultades que le atribuye la Directiva 95/46/CE en el supuesto de que una persona impugne la compatibilidad de una decisión de adecuación con la protección de la vida privada y de las libertades y derechos fundamentales de las personas.[31]

Por todo lo expuesto, el TJUE concluye que la Comisión no realizó una constatación debidamente motivada de que EEUU garantiza efectivamente un nivel de protección adecuado en razón de su legislación interna o sus compromisos internacionales, sino que se limitó a analizar únicamente el régimen del Puerto Seguro[32]. Por lo tanto, el tribunal concluye que el artículo 1 del Acuerdo vulnera las exigencias establecidas en el artículo 25.6 de la Directiva 95/46/CE.[33] Asimismo, en relación al artículo 3 del Acuerdo, el TJUE aprecia que 'la Comisión excedió los límites de la competencia que le atribuye el artículo 25.6 de la Directiva 95/46/CE'.[34] Así pues, la sentencia Schrems I declara inválidos tanto el artículo 1 como el artículo 3 de la Decisión 2000/520/CE, que, a su vez, provocan la invalidez de la Decisión de la Comisión en su conjunto. En otras palabras, el Acuerdo de Puerto Seguro se declara inválido.

2.3. Implicaciones de la sentencia Schrems I

Como señala Kuner (2017, p. 884), la sentencia Schrems I es un hito en la historia del derecho a la protección de datos en la legislación de la UE. No sólo fue la primera vez que el TJUE analizó las transferencias internacionales de datos a la luz de

[29] Apartado 89 de Schrems I.
[30] Apartado 95 de Schrems I.
[31] Apartado 102 de Schrems I.
[32] Apartado 97 de Schrems I.
[33] Apartado 98 de Schrems I.
[34] Apartado 104 de Schrems I.

disposiciones clave del derecho de la UE, como la CDFUE, sino que también reforzó notablemente el papel de las autoridades nacionales de control y definió el concepto de 'nivel adecuado de protección'. Analicemos individualmente estos elementos clave.

Como adelantábamos, Schrems I fue el primer pronunciamiento del TJUE que analiza la transferencia internacional de datos desde la perspectiva de la CDFUE. Ello es así porque la Carta se promulgó y entró en vigor con posterioridad al Acuerdo. En relación con esta Carta, también fue la primera vez que el TJUE declaró la invalidación de una norma de Derecho comunitario fundamentándose en la violación de derechos fundamentales, concretamente, el derecho al respeto de la vida privada, la protección de los datos de carácter personal y la tutela judicial efectiva (Lynskey, 2020, p. 80).[35] El empleo de esta Carta por parte del TJUE es considerado por la doctrina como un refuerzo sin precedentes del derecho a la protección de datos (Ruiz Tarrías, 2021, p. 132).

En efecto, esta sentencia viene a continuar la línea jurisprudencial del TJUE en defensa de los derechos fundamentales ante la evolución del mundo digital y frente al abuso de la vigilancia por motivos de seguridad nacional. Así, en el caso Google Spain[36], se reconoció el 'derecho al olvido' en Internet frente a los intereses económicos de los motores de búsqueda (Uría Gavilán, 2016, p. 275). En Digital Rights Ireland,[37], el TJUE anuló la Directiva 2006/24/CE, de 'conservación de datos' al considerar que sus preceptos permitían una invasión desproporcionada a los derechos reconocidos en los artículos 7 y 8 de la Carta. Esta última sentencia en concreto sirvió de inspiración para Schrems I, ya que determinó que la lucha contra los delitos graves y el terrorismo no justifica la adopción de medidas generales para almacenar los datos. El TJUE matizó que dichas medidas deben restringirse a lo estrictamente necesario, conteniendo reglas claras y precisas que regulen su alcance y aplicación. Otra sentencia que viene a ratificar las garantías que deben adoptarse frente al abuso de la vigilancia masiva es

[35] Artículos 7, 8 y 47 de la CDFUE, respectivamente.

[36] STJUE (Gran Sala), de 13 de mayo de 2014, asunto C 131/12, Google Spain, S.L., Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González.

[37] STJUE (Gran Sala), de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12. Digital Rights Ireland c. Ministerio de Comunicaciones, Marina y otros. Para un análisis de esta sentencia véase López Aguilar, J. F. (2017). La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU. *Teoría y Realidad Constitucional*, 39, pp. 557–581.

Tele2 Sverige AB[38], por la que el TJUE desarrolla las conclusiones de Digital Rigths Ireland al concretar el 'principio de estricta necesidad' (Vardanyan y Stehlik, 2020, pp. 115-116).

Por otro lado, se refuerza igualmente el papel de las autoridades nacionales de control como guardianas de los derechos fundamentales □'los superhéroes del mundo de la protección de datos' (Peers, 2015). Pese a que, como se comentó en el apartado anterior de este trabajo, el TJUE recordó la exclusividad de su facultad para declarar la invalidez de cualquier norma comunitaria, Schrems I sin duda consolida la figura de las autoridades nacionales de control, otorgándoles competencias claras y distintivas frente a una decisión de la Comisión Europea (Puerto y Sferrazza, 2017, p. 223). Además, esta sentencia fortalece su independencia. En este sentido, sigue la estela de varios fallos judiciales en los que el TJUE constató que algunos Estados Miembros habían violado los preceptos de la Directiva 95/46/CE que garantizan la total independencia en sus funciones (Uría Gavilán, 2016, p. 272).

La sentencia Schrems I es asimismo histórica por interpretar el término 'nivel adecuado de protección', ya que la Directiva 95/46/CE regulaba las decisiones de adecuación en base a ello sin entrar a definir el concepto. El TJUE establece que el término 'nivel de protección adecuado' recogido en la Directiva no significa exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la UE, sino que debe entenderse *'en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta'*.[39] Así, como sintetiza Recio Gayo (2019, p. 213), 'lo que se requiere a terceros países es un nivel sustancialmente equivalente, pero no igual, al que proporciona la legislación europea sobre protección de datos'.

Kuner (2019, p. 124) señala que gran parte de la influencia mundial de la UE en la protección de datos es gracias a la aplicación extraterritorial de la legislación de la

[38] STJUE (Gran Sala), de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB contra Post- och telestyrelsen y Secretary of State for the Home Department contra Tom Watson y otros.
[39] Apartado 73 de Schrems I.

UE. En este sentido, al reforzar el control sobre el nivel adecuado de protección de datos en terceros países (Vardanyan y Stehlik, 2020, p. 114), el caso Schrems I contribuye a expandir el 'efecto Bruselas'.[40]

Finalmente, autores como Gonzalo Domenech (2019, pp. 350-371) o Piñar Mañas (2016, pp. 442-444) destacan la relevancia de la doctrina de Schrems I en el posterior régimen jurídico de las transferencias internacionales de datos, en especial en lo referente a las decisiones de adecuación. Así, el RGPD integró esta jurisprudencia en su artículo 45 en cuestiones como los elementos a considerar por la Comisión para evaluar el nivel de protección de un tercer país, el seguimiento continuo de los acontecimientos en ese Estado que puedan afectar a la efectiva aplicación de la Decisión adoptada o la obligación de entablar consultas en el supuesto de que ya no se garantice el nivel de protección adecuado con el fin de evitar la derogación o suspensión del Acuerdo. También se ha integrado en el artículo 58 del RGPD la obligación para los Estados Miembros de facultar a las autoridades de control para poner en conocimiento de los tribunales las infracciones en materia de protección de datos y, si procede, instar acciones judiciales para hacer cumplir el Reglamento.

III. DEL ESCUDO DE PRIVACIDAD A SCHREMS II

1. EL ESCUDO DE PRIVACIDAD

Como se adelantó en la anterior sección, tras las declaraciones de Edward Joseph Snowden, la Comisión inició conversaciones con las autoridades estadounidenses para reforzar el régimen del Puerto Seguro. La sentencia Schrems I sin duda aceleró esas negociaciones, las cuales resultaron en la aprobación de un nuevo texto que sustituyó al Puerto Seguro. El nuevo Acuerdo se plasmó en la Decisión de ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE

[40] El término 'efecto Bruselas' fue acuñado por Anu Bradfor en 2012 y hace referencia a la capacidad de la UE para influir en la regulación de otros Estados o empresas a través de sus instituciones y de sus normas jurídicas. Ver Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review*, 107, (1), 1-68.

del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EEUU.

El marco normativo adoptado, conocido como el Escudo de Privacidad, fue de nuevo un sistema de autocertificación por el que las entidades estadounidenses voluntariamente se adherían al Acuerdo y se comprometían a cumplir sus principios. Este régimen era administrado y controlado por el Departamento de Comercio, el cual debía mantener y poner a disposición del público la lista de las entidades autocertificadas. A diferencia del Puerto Seguro, las empresas estaban sometidas a auditorías periódicas y debían renovar anualmente su compromiso.

Respecto a los principios del Escudo de Privacidad, éstos eran en gran medida los mismos que recogía su antecesor, salvo ciertas mejoras. Estos principios se encuentran en los párrafos 20 a 28 del nuevo Acuerdo y, a grandes rasgos, son:

1) **Principio de notificación**. De conformidad con este principio, las empresas estadounidenses estaban obligadas a informar a los particulares sobre los aspectos clave en el tratamiento de sus datos de carácter personal. Ello incluía los tipos de datos recopilados, el propósito del procesamiento de los datos, los derechos de acceso a la información y las condiciones aplicables a las transferencias ulteriores. Además, las entidades estaban obligadas a hacer públicas sus políticas de privacidad y a proporcionar enlaces al sitio web del Departamento de Comercio, a la lista del Escudo de la Privacidad y al sitio web de un proveedor adecuado de modalidades alternativas de solución de conflictos.
2) **Principio de integridad de los datos y de limitación de la finalidad**. Las entidades debían garantizar la integridad de los datos personales obtenidos y limitarse a la finalidad del tratamiento previsto. Quedaba prohibido el tratamiento de dichos datos de manera incompatible con los fines que motivaron su recogida o que el interesado hubiera aprobado posteriormente.
3) **Principio de opción**. Los interesados debían ser informados sobre la cesión de sus datos a terceros o su utilización con un fin diferente a la finalidad original y, en su caso, conferirles el derecho a oponerse.

4) **Principio de acceso**. Reconocía el derecho de los interesados a corregir, modificar o suprimir sus datos personales cuando fueran inexactos o se hubieran incumplido los principios de privacidad en su tratamiento. Asimismo, las entidades debían dar acceso a los interesados a sus datos en un plazo de tiempo razonable. El derecho de acceso sólo podía ser restringido en circunstancias excepcionales.

5) **Principio de recurso, aplicación y responsabilidad**. Las entidades adheridas al Escudo de Privacidad estaban obligadas a facilitar mecanismos de recurso independientes, eficaces y disponibles rápidamente a los particulares afectados por incumplimiento.

6) **Principio de responsabilidad de la transferencia ulterior**. Con arreglo a este principio, sólo se podían transferir datos a un tercero que actuase como Responsable o Encargado del tratamiento con fines limitados y específicos, en virtud de un contrato y únicamente si dicho contrato ofrecía el mismo nivel de protección que el garantizado por los principios.

Las mejoras que incluía el Escudo de Privacidad se pueden agrupar, según Terpan (2018, p. 1051), en tres bloques.

En primer lugar, se reforzaron los compromisos de las empresas adheridas al Acuerdo con respecto a las notificaciones, los límites a la retención de datos, los derechos de acceso y la publicidad de las políticas de privacidad. Además, el Departamento de Comercio se comprometía a llevar a cabo una supervisión continua para verificar y garantizar el cumplimiento de los compromisos asumidos por las empresas autocertificadas.

En segundo lugar, las autoridades estadounidenses proporcionaron garantías por escrito de que el acceso de las agencias de seguridad a los datos europeos estaría claramente limitado y controlado.

En tercer lugar, se garantizaba una protección efectiva de los derechos de los ciudadanos de la UE a través de una serie de mecanismos de solución de controversias en caso de violación del derecho a la protección de datos. Cabe destacar la figura del Defensor del Pueblo, nombrado por el Departamento de Estado de EEUU, cuyo

cometido era examinar posibles vulneraciones de los derechos de privacidad y protección de datos por parte de las autoridades estadounidenses.

También conviene apuntar que la Decisión 2016/1250 incluía un mecanismo de revisión periódica de la constatación de adecuación del nivel de protección garantizado por EEUU en virtud del Acuerdo. Se trataba de una revisión anual conjunta entre la Comisión y el Departamento de Comercio de EEUU que abarcaba todos los aspectos del funcionamiento del Escudo de la Privacidad, incluida la aplicación de las excepciones a los principios.

Aunque tanto el Parlamento Europeo[41] como el anterior GT29[42] acogieron favorablemente las importantes mejoras introducidas por el Escudo de Privacidad, también mostraron sus críticas ante ciertas debilidades del nuevo Acuerdo. Ambas partes manifestaron dudas sobre la independencia del Defensor del Pueblo y criticaron que no se le hubieran otorgado competencias suficientes para ejercer su función de manera eficaz. Además, señalaron que la recopilación en bloque de las comunicaciones y datos personales de los ciudadanos europeos no respondía a los criterios de necesidad y proporcionalidad establecidos en la CDFUE y que los mecanismos de recurso resultaban demasiado confusos y complejos. El Acuerdo también recibió duras críticas por parte de varios autores (Sobrino García, 2021; Gonzalo Domenech, 2019; Fahey y Terpan, 2021), quienes calificaron a la Decisión 2016/1250 como una actualización moderada del régimen anterior y destacaron que sus principios seguían sin estar a la altura de los estándares europeos respecto a la protección de datos personales (Castellanos Rodríguez, 2017; Blasi Casagran, 2017).

Se esperaba que las revisiones anuales conjuntas entre la Comisión y el Departamento de Comercio, así como las garantías proporcionadas por el gobierno de EEUU, protegiesen al Escudo de Privacidad de otra invalidación judicial (Fahey y Terpan, 2021, p. 7). Sin embargo, como se verá a continuación, lo cierto es que estas mejoras no resultaron ser suficientes.

[41] Véase Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre los flujos transatlánticos de datos (2016/2727 (RSP)).

[42] El Grupo de Trabajo del artículo 29 era el grupo de trabajo europeo independiente que se ocupó de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018, año en el que fue sustituido por el Comité Europeo de Protección de Datos (CEPD) (entrada en aplicación del RGPD). Véase Dictamen 01/2016 sobre el proyecto de Decisión sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EEUU, adoptado el 13 de abril de 2016.

2. LA INVALIDACIÓN

2.1. La invalidación del Escudo de Privacidad. Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2020 (Asunto C-311/18): Schrems II

Como consecuencia de la sentencia Schrems I, el Tribunal Superior de Irlanda anuló la desestimación de la reclamación del Sr. Schrems y se la devolvió a la autoridad de control irlandesa. En la investigación llevada a cabo por este órgano, Facebook Ireland alegó que las transferencias de datos realizadas a Facebook Inc. en EEUU se amparaban en las cláusulas tipo recogidas en el anexo de la Decisión de la Comisión 2010/87/UE, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los Encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46, conocidas como Decisión CPT[43].

A instancia de la autoridad de control irlandesa, el 1 de diciembre de 2015, el Sr. Schrems presentó una reclamación modificada y alegó que el Derecho de EEUU obliga a Facebook Inc. a poner a disposición de las autoridades estadounidenses los datos personales que se le transfieren. En su opinión, estos datos son tratados en el marco de programas de vigilancia de una manera incompatible con los artículos 7, 8 y 47 de la CDFUE y, por ello, el Sr. Schrems solicitó la prohibición o suspensión de la transferencia de sus datos personales a EEUU.

La autoridad de control de Irlanda consideró que la nueva reclamación planteaba la cuestión de la validez de la Decisión CPT por lo que, apoyándose en la jurisprudencia resultante de Schrems I, inició un procedimiento ante el Tribunal Superior irlandés. Finalmente, el 4 de mayo de 2018, este Tribunal plantea once cuestiones prejudiciales que son resueltas por el TJUE en la sentencia Schrems II, tal y como se analiza a continuación.

[43] Decisión de la Comisión 2010/87/UE, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46 (DO 2010, L 39, p. 5), en su versión modificada por la Decisión de Ejecución (UE) 2016/2297 de la Comisión, de 16 de diciembre de 2016 (DO 2016, L 344, p. 100).

2.1.1. Sobre el ámbito de aplicación del RGPD al tratamiento de datos personales con fines de seguridad nacional

En la primera cuestión prejudicial, el Tribunal Superior de Irlanda pregunta acerca de la aplicabilidad del RGPD a las transferencias de datos personales realizadas con fines comerciales a un operador económico establecido en un tercer país desde un Estado Miembro cuando esos datos puedan ser tratados por las autoridades del tercer país en cuestión con fines de seguridad nacional, defensa y seguridad del Estado.

El TJUE confirma que el RGPD resulta aplicable a una transferencia de estas características.[44] Para llegar a esta conclusión, el TJUE analiza primero los artículos 2.1 y 2.2 del Reglamento. A este respecto, como ya se había reconocido en la sentencia Schrems I, se indica que la 'operación consistente en hacer transferir datos personales desde un Estado Miembro a un tercer país constituye por sí misma un tratamiento de datos personales, en el sentido del artículo 4. 2 del RGPD', el cual define 'tratamiento' como cualquier operación realizada sobre datos personales.[45] Por otra parte, se apunta a que la transferencia se realizó 'entre Facebook Ireland hacia Facebook Inc., es decir, entre dos personas jurídicas', por lo que no está comprendida dentro de ninguna de las excepciones al ámbito de aplicación del RGPD conforme al artículo 2.2 del mismo.[46] Asimismo, el TJUE recuerda que este Reglamento es de aplicación a las transferencias internacionales de datos conforme a su capítulo V.[47]

2.1.2. Sobre el nivel de protección adecuado para las transferencias de datos a terceros países basadas en cláusulas tipo

Este grupo sistémico responde a las cuestiones prejudiciales segunda, tercera y sexta planteadas acerca de cuál es el nivel de protección exigido en los artículos 46.1 y 46.2 letra c del RGPD en el marco de una transferencia internacional de datos basada en

[44] Apartado 89 de Schrems II.
[45] Apartado 83 de Schrems II.
[46] Apartado 85 de Schrems II.
[47] Apartado 82 de Schrems II.

cláusulas tipo. El Tribunal Superior de Irlanda también solicita que se precise cuáles son los elementos a tener en cuenta para realizar dicha evaluación.

Respecto al nivel de protección exigido, el TJUE comienza haciendo una lectura conjunta de los artículos 46.1 y 46.2 RGPD. De esta lectura se desprende que cuando no existe una decisión de adecuación *'el Responsable o el Encargado del tratamiento sólo podrá transmitir datos personales a un tercer país si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas*', pudiendo proporcionarse esas garantías adecuadas, en particular, mediante cláusulas tipo de protección de datos adoptadas por la Comisión.[48] Sin embargo, el TJUE matiza a continuación que el artículo 46 RGPD no precisa cuál es la naturaleza de las exigencias que se derivan de esa referencia a las 'garantías adecuadas, a los derechos exigibles y a las acciones legales efectivas'.[49]

Tras realizar una lectura interdependiente de las disposiciones del capítulo V del RGPD, que expondremos en el siguiente apartado, el TJUE interpreta que dichas garantías adecuadas '*deben asegurar que las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gocen, como en el marco de una transferencia basada en una decisión de adecuación, de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión*'.[50]

Respecto a los elementos a tomar en consideración para determinar la adecuación del nivel de protección en el contexto de una transferencia de datos basada en cláusulas tipo, el TJUE precisa que se tendrá en cuenta tanto las estipulaciones contractuales acordadas entre el Responsable o el Encargado del tratamiento establecidos en la Unión y el destinatario de la transferencia establecido en el país tercero de que se trate como los elementos pertinentes del sistema jurídico de dicho país**.** Los elementos a los que se refiere se corresponden con los mencionados, de modo no exhaustivo, en el artículo 45.2 del RGPD.[51]

[48] Apartado 91 de Schrems II.
[49] Apartado 92 de Schrems II.
[50] Apartado 96 de Schrems II.
[51] Apartado 104 de Schrems II.

2.1.3. Sobre las autoridades de control

En la octava cuestión prejudicial, se solicita al TJUE que se pronuncie sobre si la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos personales a un país tercero basada en cláusulas tipo de protección de datos adoptadas por la Comisión cuando consideren que en ese tercer país no se puede garantizar un nivel de protección adecuado. Al evaluar este supuesto, el TJUE señaló que las autoridades de protección de datos nacionales son las encargadas del control del cumplimiento del RGPD, están investidas de competencia para comprobar si una transferencia de datos personales respeta las exigencias de las normas de la UE y disponen de importantes poderes de investigación para tratar las reclamaciones que se le presenten.[52] Por todo esto, el TJUE resuelve que, a no ser que exista una decisión de adecuación, la autoridad de control está obligada '*a suspender o prohibir una transferencia de datos personales a un país tercero si considera, a la luz de todas las circunstancias que rodean a esa transferencia, que las cláusulas tipo de protección de datos no se respetan o no pueden ser respetadas en ese país tercero y que la protección de los datos transferidos exigida por el Derecho de la Unión no puede garantizarse mediante otros medios, si el Responsable o el Encargado del tratamiento establecidos en la Unión no ha suspendido la transferencia o puesto fin a esta por sí mismos.*'[53]

En la novena cuestión prejudicial, el Tribunal Superior de Irlanda solicita que se dilucide si una autoridad de control de un Estado Miembro está vinculada al Acuerdo del Escudo de Privacidad. El TJUE responde, recordando la jurisprudencia de la sentencia Schrems I, que mientras que la decisión de adecuación no sea invalidada, las autoridades de control no pueden adoptar medidas contrarias a esa decisión.[54] Por lo tanto, no pueden suspender o prohibir una transferencia de datos personales a una entidad que se haya adherido al Escudo aunque consideren que el tercer país de que se trate no garantiza un nivel de protección suficiente.[55]

[52] Apartados 107, 108 y 111 de Schrems II.
[53] Apartado 121 de Schrems II.
[54] Apartado 18 de Schrems II.
[55] Apartado 156 de Schrems II.

2.1.4. Sobre la validez de la Decisión 2010/87/UE

El TJUE responde a las cuestiones prejudiciales séptima y undécima en referencia a la validez de la Decisión CPT. Concretamente, el Tribunal Superior de Irlanda cuestiona si esta Decisión puede garantizar un nivel de protección adecuado, dado que las cláusulas tipo de protección de datos que prevé no son vinculantes para las autoridades de terceros países.

El TJUE indica que, debido al carácter contractual de las cláusulas tipo de protección de datos recogidas en una decisión de la Comisión, éstas no pueden vincular a las autoridades públicas de terceros países, ya que no son partes del contrato, pero ello no conlleva la invalidez de la Decisión CPT.[56] En cambio, el TJUE precisa que la validez de la Decisión CPT depende de si *'incluye mecanismos efectivos que permitan en la práctica garantizar que el nivel de protección exigido por el Derecho de la Unión sea respetado y que las transferencias de datos personales basadas en esas cláusulas sean suspendidas o prohibidas en caso de violación de dichas cláusulas o de que resulte imposible su cumplimiento'*.[57]

El análisis de los concretos mecanismos de esta Decisión llevó al TJUE a determinar su validez dado que, en primer lugar, establece la obligación -tanto para el exportador de los datos como para el destinatario de la transferencia- de comprobar con carácter previo que el país tercero de que se trate respeta del nivel de protección exigido por el Derecho de la Unión.[58] En segundo lugar, el destinatario está obligado a informar al exportador de su eventual incapacidad para cumplir con esas cláusulas, incumbiendo entonces a este último suspender la transferencia de datos o rescindir el contrato. [59] Por último, el exportador está obligado a notificar a la autoridad de control competente en el supuesto de que decida no suspender la transferencia aun cuando existan circunstancias que puedan tener un importante efecto negativo sobre las garantías ofrecidas y las obligaciones impuestas.[60]

[56] Apartados 125 y 136 de Schrems II.
[57] Apartado 137 de Schrems II.
[58] Apartado 142 de Schrems II.
[59] Apartado 142 de Schrems II.
[60] Apartado 145 de Schrems II.

No obstante, aun cuando las cláusulas tipo sean válidas, el TJUE entiende que existen determinadas situaciones en el tercer país de que se trate en las que no se puede garantizar la protección de datos necesaria basándose únicamente en dichas cláusulas. En particular y en clara alusión a EEUU 'esto sucede cuando el Derecho de ese tercer país permite a sus autoridades públicas llevar a cabo injerencias en los derechos de los interesados relativos a sus datos'.[61] Ante estas situaciones, el TJUE insta al Responsable del tratamiento a adoptar medidas adicionales con el fin de garantizar el respeto del nivel de protección exigido por el Derecho de la UE.[62]

2.1.5. Sobre la validez del Escudo de Privacidad

Conviene puntualizar que el Escudo de Privacidad se adoptó con posterioridad al inicio de este procedimiento judicial. No obstante, aunque las cuestiones prejudiciales cuarta y quinta giran en torno a la validez de la Decisión CPT, el TJUE considera oportuno entrar a examinar si la Decisión 2016/1250 se ajusta a las exigencias derivadas del RGPD entendido a la luz de la CDFUE.[63] Además, el Tribunal irlandés pregunta en la décima cuestión si la protección exigida por el artículo 47 de la Carta queda garantizada por medio del Defensor del Pueblo.[64]

Respecto al contenido de la Decisión 2016/1250, la Sentencia comienza poniendo de manifiesto que aunque la Comisión constató en su artículo 1 que EEUU garantiza un nivel de protección adecuado, el Acuerdo también precisa que la adhesión a sus principios puede verse limitada, en particular, por exigencias de seguridad nacional, interés público y cumplimiento de la Ley.[65] Así pues, se repite el mismo escenario que en el Acuerdo del Puerto Seguro, por lo que, siguiendo el criterio de Schrems I[66], el TJUE considera que la primacía de las referidas exigencias posibilita la injerencia de las autoridades públicas estadounidenses en los derechos fundamentales de las personas cuyos datos personales se transfieren. Más concretamente, dichas

[61] Apartado 126 de Schrems II.
[62] Apartado 133 de Schrems II.
[63] Apartado 161 de Schrems II.
[64] Apartados 150 y 151 de Schrems II.
[65] Apartados 163 y164 de Schrems II.
[66] Apartado 164 de Schrems II.

injerencias se producen como consecuencia del acceso y tratamiento de los datos personales transferidos desde la UE a EEUU 'en el marco de los programas de vigilancia *PRISM* y *Upstream* basados en el artículo 702 del FISA[67] y en la EO 12333[68]'.[69]

Siguiendo con el contenido de la Decisión 2016/1250, el TJUE también recuerda que la Comisión, en el Considerando 140 tras analizar 'la información disponible acerca del ordenamiento jurídico de los Estados Unidos, incluidas las declaraciones y compromisos prestados por el Gobierno estadounidense', opina que las injerencias de los poderes públicos en los derechos fundamentales de los ciudadanos europeos en el marco de una transferencia realizada al amparo del Escudo de Privacidad, 'se limitarán a lo estrictamente necesario para alcanzar el objetivo legítimo perseguido, y que existe una tutela judicial efectiva frente a tales injerencias'. [70] Sin embargo, como se expone a continuación, la Comisión erró en ambas cuestiones.

El TJUE reiteradamente ha declarado que la comunicación de datos de carácter personal a un tercero, como una autoridad pública, constituye una injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la CDFUE.[71] Estos derechos no constituyen prerrogativas absolutas, pero cualquier limitación deberá respetar su contenido esencial, ser necesaria y de interés general. Con el fin de respetar el principio de proporcionalidad, cualquier norma que limite estos derechos 'deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario'.[72] Tras realizar un análisis del artículo 702 del FISA y de la EO 12333, el TJUE pone de relieve que estas normas confieren un poder extremadamente amplio a las autoridades públicas estadounidenses, sin límites para la ejecución de programas de vigilancia con fines de inteligencia exterior, ni garantías para las personas no nacionales de EEUU.[73] Todo ello refleja que esta normativa no 'satisface las exigencias mínimas establecidas por el Derecho de la Unión con respecto al principio de proporcionalidad, de modo que (…) no se limitan a lo estrictamente

[67] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-11 et sq. (1978).
[68] Executive Order 12333. United States Intelligence Activities (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)).
[69] Apartado 165 de Schrems II.
[70] Apartado 167 de Schrems II.
[71] Apartado 171 Schrems II.
[72] Apartados 172-176 de Schrems II.
[73] Apartados 180 y 181 de Schrems II.

necesario'.[74] Por consiguiente, queda demostrado que la Comisión, al declarar que EEUU garantiza un nivel adecuado de datos personales, no tuvo en cuenta las exigencias resultantes del artículo 45 del RGPD, interpretado a la luz de los artículos 7 y 8 de la CDFUE. Por lo tanto, el TJUE resuelve que el artículo 1 de la Decisión es inválido.[75]

Con respecto al derecho a la tutela judicial efectiva recogido en el artículo 47 de la CDFUE, el TJUE considera que la Comisión también debe constatar su respeto a la hora de evaluar el nivel de protección adecuado del tercer país.[76] Sin embargo, del análisis pormenorizado de las normas de vigilancia masiva, se desprende que no confieren a los ciudadanos europeos derechos exigibles a las autoridades estadounidenses ante los tribunales, de modo que se les priva de tutela judicial efectiva.[77] En lo que se refiere al Defensor del Pueblo, el TJUE entiende que esta figura tampoco respeta el artículo 47 de la CDFUE.[78] Por una parte, la Decisión 2016/1250 no contiene ninguna indicación sobre sus facultades para obligar a los servicios de inteligencia a corregir las infracciones detectadas en el ámbito del Escudo de Privacidad 'ni tampoco menciona ninguna garantía legal que acompañe a ese compromiso y pueda ser invocada por los interesados'.[79] Por otra parte, carece de garantías sobre su independencia con respecto al poder ejecutivo dado que es nombrado por el Secretario de Estado y forma parte integrante del Departamento de Estado.[80]

Por todo lo expuesto, el TJUE concluye que la Decisión 2016/1250 es inválida. Dicho de otro modo, se pone fin al Escudo de Privacidad.

[74] Apartado 184 de Schrems II.
[75] Apartado 199 de Schrems II.
[76] Apartado 186 de Schrems II.
[77] Apartado 192 de Schrems II.
[78] Apartado 197 de Schrems II.
[79] Apartado 196 de Schrems II.
[80] Apartado 196 de Schrems II.

2.2. Consecuencias de Schrems II en las transferencias internacionales de datos personales

Muchos autores, como Francesca Bignami (2020), han calificado la sentencia Schrems II como una especia de secuela. 'Mismas partes, misma autoridad de control de datos irlandesa, los mismos programas de inteligencia estadounidenses' y, de nuevo, la invalidación del Acuerdo que servía como base jurídica para las transferencias de datos personales transatlánticas por no garantizar un nivel adecuado de protección de datos a los ciudadanos europeos en caso de acceso de los poderes públicos de EEUU (Bignami, 2020). Por su parte, Kenneth Propp y Peter Swire (2020) describen la Sentencia como 'el último capítulo de una larga y enredada historia de litigios ante tribunales irlandeses y europeos sobre la intersección de los derechos de privacidad de la UE y la ley de vigilancia de EEUU' en el que el TJUE recuerda que la protección otorgada a los datos personales en el RGPD debe acompañar a los datos cuando éstos 'viajan al extranjero', aunque allí sean tratados por sus autoridades públicas con fines de seguridad nacional (Kenneth y Swire, 2020).

Sin embargo, como apunta Theodore Christakis (2020), 'Schrems II va mucho más allá de Schrems I'. El TJUE no sólo invalida el Escudo de Privacidad, sino que realiza un desarrollo del régimen teórico de protección de las transferencias de datos personales que va a establecer el mismo estándar de protección independientemente del instrumento legal que se emplee (Christakis, 2020). La doctrina coincide en señalar que este desarrollo es de los aspectos más novedosos y significativos de la sentencia. Así, Schrems II va a tener una gran repercusión en la futura regulación de las transferencias internacionales de datos basadas en alguna de las garantías adecuadas del artículo 46 del RGPD. El TJUE, como veremos a continuación, hará una reinterpretación del Reglamento para definir el nivel de protección adecuado de los datos personales y determinar cuáles son las obligaciones de los sujetos implicados en una transferencia de este tipo. Asimismo, se pronunciará sobre las facultades de las autoridades de control en este contexto (Kuner 2020; Ruiz Tarrías, 2021; Costello, 2020, Ortega Giménez y García Escobar, 2020). Por último, aparte del impacto en la interpretación del artículo 46 del RGPD, Schrems II también influirá a las futuras decisiones de adecuación en el ámbito comercial.

2.2.1. Nivel de protección adecuado

Recordemos que, tradicionalmente, se ha interpretado que el artículo 45 del RGPD requiere como requisito para realizar una transferencia de datos personales que el tercer país en cuestión tenga un nivel adecuado de protección de datos, evaluación que se realizará teniendo en cuenta los elementos enunciados en su segundo apartado. Por su parte, el artículo 46 del RGPD requiere garantías adecuadas a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. Sin duda, estos requisitos son diferentes a los del artículo 45. Sin embargo, en Schrems II, el Tribunal sostuvo, en primer lugar, que el estándar de 'equivalencia esencial' con la legislación de la UE se aplica a las garantías adecuadas del artículo 46[81] del mismo modo que si de una decisión de adecuación se tratase y, en segundo lugar, que la evaluación en ambos casos se hará conforme a los elementos del artículo 45.2 del RGPD.[82]

Para alcanzar esta conclusión, el TJUE leyó los artículos 45 y 46 del RGPD de manera complementaria e importó al artículo 46 los elementos del artículo 45.2, los cuales han de ser tenidos en cuenta al evaluar la adecuación del nivel de protección. El TJUE justificó la lectura del artículo 46 a la luz del artículo 45 al señalar que el artículo 46 no precisa cuál es la naturaleza de los requisitos que se derivan de su redacción[83], pero al figurar en el capítulo V del RGPD, debe interpretarse a la luz del artículo 44 del RGPD, titulado 'Principio general de las transferencias'. Este principio establece que 'todas las disposiciones de dicho capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por dicho Reglamento no se vea menoscabado' (Costello, 2020, p. 1053). Cabe destacar aquí que las recomendaciones publicadas el 10 de noviembre de 2020 por el CEPD aclaran que, aunque el TJUE interpretó el artículo 46.1 del RGPD en el contexto de la validez de las cláusulas contractuales tipo, su interpretación se aplica a toda transferencia a terceros países basada en cualquiera de las herramientas mencionadas en el artículo 46 del RGPD.[84]

[81] Apartado 96 de Schrems II.
[82] Apartado 104 de Schrems II.
[83] Como ya señalamos en el análisis de la sentencia Schrems II, el artículo 46 del RGPD no precisa la naturaleza de las exigencias que se derivan de esa referencia a las 'garantías adecuadas', a los 'derechos exigibles' y a las 'acciones legales efectivas' (apartado 92 de Schrems II).
[84] Ver la página 5 de las Recomendaciones 02/2020 sobre las garantías esenciales europeas para medidas de vigilancia adoptadas 10 de noviembre de 2020 por el CEPD.

2.2.2. Responsabilidad de las partes de la transferencia

Volviendo al RGPD, el artículo 45 establece que la Comisión es el órgano encargado de realizar la evaluación del nivel de protección de datos del tercer país. En Schrems II, como ya se ha apuntado en el análisis de la sentencia, cuando se trate de transferencias basadas en algún instrumento del artículo 46, el TJUE determina que será el Responsable o el Encargado del tratamiento establecidos en la UE quienes deben realizar dicha evaluación y, en su defecto, lo harán las autoridades de control.[85] Como señala Costello (2020, p. 1053), esta situación va a crear un sistema paralelo de 'mini decisiones de adecuación' *ad hoc* elaboradas por los Responsables de las transferencias. En palabras de Rodríguez Ayuso (2021, p.342), 'esto supone, *de facto*, una traslación de la responsabilidad hacia el Responsable del tratamiento'.

Como determina el TJUE y aclara el CEPD,[86] el exportador y el destinatario de los datos personales están obligados a evaluar, antes de realizar la transferencia internacional, si algún elemento del Derecho o la práctica del tercer país puede afectar a la eficacia de las garantías adecuadas del instrumento de transferencia que se emplee, en el contexto de la transferencia específica. Deberán prestar especial atención a aquellas leyes que puedan establecer requisitos para divulgar datos personales a las autoridades públicas o que concedan a dichas autoridades poderes de acceso a los datos personales. También se evaluará si el tercer país dispone de mecanismos eficaces para que los ciudadanos europeos puedan acceder a un recurso judicial contra el acceso ilegal de las autoridades a sus datos personales.

Una vez realizada la evaluación, si las partes consideran que la transferencia podría suponer el menoscabo de alguno de los derechos de protección de datos del titular objeto de la misma, deberán valorar la inclusión de medidas complementarias que, junto a las garantías contenidas en los mecanismos de transferencia del artículo 46 del RGPD, permitan garantizar en la práctica el mismo nivel de protección otorgado por el RGPD.

[85] Apartado 134 de Schrems II.

[86] Ver Preguntas frecuentes sobre la Sentencia del Tribunal de Justicia de la Unión Europea en el asunto C 311/18- Comisaria de Protección de Datos vs Facebook Irlanda y Maximillian Schrems. Adoptada el 23 de julio de 2020 (pp.1-3) y Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE. Adoptadas el 10 de noviembre de 2020 (pp.13-18, 24-39).

Ni el RGPD ni la sentencia especifican cuáles podrían ser esas medidas complementarias, por lo que el CEPD dictó posteriormente las Recomendaciones 01/2020 adoptadas el 10 de noviembre de 2020 que, además de proporcionar a los exportadores una guía para realizar las transferencias internacionales, otorga algunos ejemplos de medidas complementarias que podrían aplicarse. Este documento habla de medidas técnicas, medidas contractuales adicionales y medidas organizativas. La relación no es exhaustiva y podrán usarse una o varias medidas si fuese necesario. Seleccionar el instrumento de transferencia más adecuado para la transferencia, así como las medidas complementarias, será una acción que el Responsable realizará caso por caso. Aunque la sentencia no lo menciona, esta obligación es una manifestación del 'principio de responsabilidad proactiva' del artículo 5.2 del RGPD, el cual exige que los Responsables del tratamiento sean responsables y capaces de demostrar el cumplimiento de los principios del RGPD relativos al tratamiento de datos personales.

Por último, en el supuesto de no encontrar o de no poder aplicar una medida complementaria que garantice la protección de los datos transferidos, el Responsable deberá suspender o poner fin a la transferencia. Si, a pesar de esto, el Responsable decide continuar con la transferencia, deberá notificarlo a la autoridad de control. Ésta suspenderá o prohibirá la transferencia en aquellos casos en los que se considere que no se puede garantizar un nivel de protección esencialmente equivalente al Derecho de la UE.

Según Theodore Christakis (2020), el desarrollo del capítulo V del RGPD que realiza Schrems II propone, en teoría, un régimen más integral y coherente de protección de datos**.** Este autor comparte la opinión de aquéllos que creen que las cláusulas tipo eran una 'mera formalidad' o 'ficción legal', un instrumento 'insuficiente si la ley de otro país requiere o permite el acceso a datos personales en contra de las garantías del RGPD'. Un ejemplo de ello serían las transferencias mediante cláusulas tipo hacia China, donde la protección de datos personales frente al gobierno es esencialmente inexistente. Al exigir que tanto los exportadores de datos como las autoridades de control velen por que se apliquen a las garantías adecuadas del artículo 46 del RGPD la misma protección que tiene una transferencia de datos amparada por una decisión de adecuación, el TJUE evita 'la trampa del doble rasero'. Christakis (2020) opina que esto aporta coherencia al sistema legal y permite garantizar la equidad

en el trato a cualquier tercer país. Sin embargo, este autor también reconoce que este nuevo régimen genera mucha incertidumbre en la práctica.

Una de las principales preguntas que surge tras Schrems II es cómo podrán las empresas ser capaces de realizar un análisis del Derecho de terceros países si la propia Comisión, con todos sus medios, demostró estar equivocada dos veces en relación con tales evaluaciones, una vez con el Puerto Seguro y otra con el Escudo de Privacidad (Christakis, 2020). Esta dificultad de las empresas para conocer en profundidad la legislación y las políticas de otros países se suma al aumento significativo de tanto los costes como el volumen de trabajo, lo cual perjudica especialmente a las pequeñas y medianas empresas (Fuentes Máiquez, 2020, p. 110).

Otra cuestión sobre la que se debe arrojar luz es cuál debe ser la forma y el contenido de las medidas que complementan los instrumentos de transferencia para asegurar el cumplimiento del nivel de protección de datos personales para la UE. Como señala Kuner (2020), el TJUE aprobó el uso de las cláusulas tipo de la Decisión CTT basándose en que las protecciones que brindan no se basan en el sistema legal del tercer país de transferencia -como ocurre cuando existe una decisión de adecuación- sino en las protecciones que brinda el Responsable y que sirven para compensar la falta de protección de datos en el lugar de destino. Sin embargo, como ya hemos adelantado, Schrems II no se pronuncia sobre el contenido de estas medidas y las Recomendaciones publicadas el 10 de noviembre de 2020 por el CEPD sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE tampoco clarifican excesivamente la cuestión.

Para acabar con la inseguridad jurídica que resulta tras la invalidez del Escudo de Privacidad, la doctrina sugiere que el CEPD tome un papel más activo. En primer lugar, proporcionando evaluaciones de adecuación centralizadas ya a *priori* que establezcan cuándo y cómo se pueden operar las transferencias de datos bajo cláusulas tipo en ausencia de una decisión de adecuación y, en segundo lugar, precisando el contenido de las medidas complementarias (Christakis, 2020).

2.2.3. Autoridades de control de datos

En Schrems II, el TJUE se pronunció a favor de una mayor implicación de las autoridades de control de datos en el contexto de las transferencias a terceros países. Bignami (2020) destaca que son el 'respaldo esencial' para las transferencias basadas en contratos a terceros países. El TJUE les ha otorgado la función de supervisar las evaluaciones de los terceros países que realizan las empresas. En aquellos casos en los que consideren que no se pueda garantizar un nivel de protección de datos sustancialmente equivalente al de la UE, deberán suspender o prohibir la transferencia. Sin embargo, es cuestionable otorgar esta actividad a las autoridades de control ya que ni son expertas en leyes de vigilancia extranjera ni cuentan con personal suficiente (Bignami, 2020 y Christakis, 2020).

En definitiva, el desarrollo del capítulo V del RGPD respecto a las transferencias internacionales de datos ha dado lugar a un sistema de investigación del nivel de protección de datos de los terceros países en capas (Costello, 2020, p. 1056). En un primer nivel, se encuentran las decisiones de adecuación de la Comisión. En segundo lugar, las 'mini decisiones de adecuación' *ad hoc* de los Responsables y Encargados de las transferencias de datos. Por último, la supervisión ejercida por las autoridades de control sobre estos últimos.

2.2.4. Futuras decisiones de adecuación

Una última consecuencia por destacar de la sentencia Schrems II es su impacto en las futuras decisiones de adecuación. En concreto, en el ámbito comercial. Esto es porque el TJUE incluye en la evaluación de la Comisión el eventual control de los ulteriores tratamientos a los que los datos objeto de la transferencia puedan verse expuestos como consecuencia de la misma si la relación que justifica la transferencia es una relación comercial (Cordero Álvarez, 2022). Ello sin prejuicio de que el ulterior tratamiento sea por parte de las autoridades públicas del tercer Estado y esté justificado en razones de seguridad pública, defensa o seguridad.

Este nuevo compromiso adoptado por la Comisión tras la sentencia Schrems II va a condicionar su evaluación en las decisiones de adecuación, así como en sus posteriores labores de seguimiento (Cordero Álvarez, 2022).

IV. LAS TRANSFERENCIAS INTERNACIONALES ENTRE LA UE Y EEUU TRAS LA INVALIDEZ DEL ESCUDO DE PRIVACIDAD

1. SITUACIÓN ACTUAL

La consecuencia inmediata derivada de la Sentencia Schrems II fue la invalidez del Escudo de Privacidad, situando a EEUU en la misma posición que cualquier otro tercer país que no cuente con una decisión de adecuación de la Comisión. A diferencia de Schrems I, Schrems II no otorgó un período de gracia, sino que sus efectos fueron inmediatos. El TJUE consideró que la anulación del Acuerdo no creaba un vacío legal al existir la posibilidad de poder recurrir al artículo 49 del RGPD. Éste recoge las excepciones en las que se puede realizar una transferencia internacional de datos en ausencia de una decisión de adecuación o de garantías adecuadas en virtud del artículo 46 del RGPD.[87] El CEPD justificó esta decisión del TJUE alegando que 'la legislación estadounidense evaluada por el TJUE no proporciona un nivel de protección sustancialmente equivalente al garantizado en la UE'.[88]

Así pues, en ausencia del Escudo de Privacidad, los principales mecanismos disponibles para las transferencias de datos personales entre la UE a EEUU son las cláusulas contractuales tipo y las normas corporativas vinculantes. Estos mecanismos eximen a los exportadores de datos de las obligaciones generales de solicitud de autorización y notificación previa a la operación de transferencia ante las autoridades nacionales de control (Cordero Álvarez, 2022).

[87] Apartado 202 de Schrems II.
[88] Ver Preguntas frecuentes sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18- Comisaria de Protección de Datos vs Facebook Irlanda y Maximillian Schrems. Adoptada el 23 de julio de 2020, pp. 2-3.

En junio de 2021, la Comisión publicó unas nuevas cláusulas contractuales tipo que sustituyeron a los modelos vigentes, de 2001 y 2010.[89] La Decisión de Ejecución 2021/914 de la Comisión de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el RGPD, intenta solventar las deficiencias señaladas en Schrems II a la vez que adapta los contratos a las exigencias del RGPD. Estas cláusulas integran el principio de responsabilidad proactiva y amplían el ámbito de aplicación de las cláusulas tipo. A diferencia de los modelos anteriores, que sólo regulaban la relación entre Responsable y Responsable y entre Responsable y Encargado, las nuevas cláusulas también regulan la relación entre Encargado y Encargado y entre Encargado y Responsable (Cordero Álvarez, 2022).

En cualquier caso, la suscripción de alguno de los instrumentos que ofrecen garantías adecuadas previstas en el artículo 46 del RGPD no resulta suficiente pues, como ha señalado el CEPD, el TJUE consideró que el artículo 702 del FISA y la EO 12333 se aplican a cualquier transferencia a los EEUU, independientemente del instrumento de transferencia empleado. Por esta razón, como se ha estudiado en el apartado anterior, es preciso que el exportador de datos, en su caso ayudado por el importador, analice el impacto que la legislación de EEUU pueda tener en el nivel de protección proporcionado, de manera que éste sea en lo esencial equivalente al Derecho de la UE. En relación con esto, en noviembre de 2020, el CEPD publicó unas nuevas recomendaciones que tienen como objeto proporcionar elementos para examinar si las medidas de vigilancia que permiten el acceso a datos personales por parte de las autoridades públicas de un tercer país se pueden considerar o no una injerencia justificable.[90]

Como se puede comprobar, cualquiera de las opciones disponibles dista mucho de la sencillez que aporta el marco jurídico de una decisión de adecuación. Además de la complejidad del proceso al que se han de enfrentar las empresas, no olvidemos que pueden darse situaciones en las que resulte imposible realizar una transferencia internacional de datos personales.

[89] Decisión 2001/497/CE y Decisión 2010/87/UE.
[90] Ver Recomendaciones 02/2020 sobre las garantías esenciales europeas para medidas de vigilancia. Adoptadas el 10 de noviembre de 2020.

1.1. Implicaciones para las empresas

Las consecuencias de Schrems II y su doctrina pueden reducir sensiblemente el tráfico de datos entre la UE y EEUU, lo cual podría afectar negativamente a su relación comercial. Un estudio realizado estima que la invalidación del Escudo de Privacidad podría reducir el comercio de servicios digitales entre un 5% y un 6%. Esto supondría una reducción del PIB de la UE de entre un 0,14% y un 0,22% (European Centre for International Political Economy and Kearney Global Business Policy Council, 2021, p. 33).

En junio de 2021, varias asociaciones empresariales españolas relacionadas con el mundo digital publicaron una carta abierta demandando una solución política para preservar las transferencias de datos entre la UE y EEUU. Alegaban que las consecuencias de Schrems II afectarían al desarrollo económico, social y científico español ya que depende en gran medida de la cooperación y del flujo de datos global. También aseguraban que la inseguridad jurídica resultante ya estaba entorpeciendo el comercio, suponiendo una desventaja competitiva para las empresas españolas y europeas en una economía globalizada.[91] Estas manifestaciones bien podrían ser el reflejo de los empresarios de cualquier otro Estado Miembro.

Cabe tener en cuenta que la mayoría de los prestadores de servicios digitales tienen su sede en EEUU, por lo que cualquier transferencia de datos, aunque se haga entre Estados Miembros, puede acabar en EEUU y, por ende, en manos de las autoridades públicas estadounidenses. Entre los servicios utilizados, podemos encontrar desde las redes sociales, servicios de *mailing*, de videollamadas y sistemas operativos hasta la computación en la nube, que hoy en día se ha convertido en una herramienta imprescindible para la mayoría de las empresas. Esto pone de relieve la magnitud del problema agravado actualmente por la pandemia mundial del Covid-19, que vino a acelerar el proceso de digitalización del mundo en el que vivimos.

Al otro lado del Atlántico, las grandes tecnológicas estadounidenses también se han enfrentado a duras dificultades durante estos últimos dos años sin Acuerdo. Microsoft ha sido la primera en guardar todos los datos personales de los usuarios

[91] Este documento se puede consultar en https://ametic.es › files › *carta abierta privacy shield*.

europeos en servidores dentro de la UE (Pérez, 2021). Amazon se enfrenta en Alemania a una demanda interpuesta en 2020 por continuar transfiriendo datos a EEUU sobre la base del invalidado Escudo de Privacidad (Cordero Álvarez, 2022).[92] Meta incluso manifestó la posibilidad de no poder ofrecer sus servicios de Facebook, WhatsApp o Instagram si no había un nuevo acuerdo transatlántico. Algunos medios lo entendieron como una amenaza de irse de Europa, pero la empresa de Mark Zuckerberg rápidamente lo desmintió, aunque exigiendo normas claras y globales para proteger los flujos de datos a largo plazo (Bracero, 2022). Amenaza o falta de ésta, la realidad es que la gestión de las transferencias de datos se vuelve cada vez más compleja.

Otro ejemplo de ello lo encontramos en las recientes decisiones de las autoridades de control de Austria y Francia respecto a Google Analytics. Esta herramienta de Google emplea una *cookie* que realiza estadísticas con relación al uso que hace el usuario de Internet y que sirven a los propietarios de las páginas webs para obtener información de sus lectores. El problema es que esos datos pueden acabar en la sede de Google en EEUU y por esta razón las autoridades han determinado que el uso de este programa sin las debidas garantías adicionales constituye una transferencia ilegal de datos conforme al RGPD (Economist & Jurist, 2022).

1. PERSPECTIVAS DE FUTURO

La importancia económica de la relación transatlántica y la necesidad de aportar seguridad jurídica a la gestión de las transferencias internacionales de datos requiere que la UE y EEUU se involucren en un tercer intento de crear un marco jurídico estable capaz de soportar un Schrems III. Schwartz y Peifer (2017, p. 157) señalan que, para encontrar un camino a seguir, es necesario comprender la base de las diferencias entre ambas potencias con respecto a la privacidad. Por esta razón, conviene ahondar un poco más en las diferencias que se señalaron al inicio de este trabajo para continuar planteando los retos de un posible tercer acuerdo y terminar con soluciones alternativas aportadas por la doctrina.

[92] A fecha de realización del presente trabajo, la demanda contra Amazon todavía no ha sido resuelta.

2.1. Diferencias fundamentales entre las políticas de privacidad

Schrems II demostró por segunda vez, y en menos de cinco años, el choque entre los valores europeos del respeto a la privacidad y a la protección de datos contra la defensa de la vigilancia por parte de EEUU. James Q. Whitman (2004, p. 1161) afirma que existen 'dos culturas occidentales de la privacidad'. Mientras en la UE entendemos la privacidad como un concepto basado en la dignidad y el honor personal, en EEUU se asocia al concepto de libertad. Esta diferencia es la clave para entender cómo se asimiló de manera tan diferente el impacto del terrorismo global del que fueron víctimas ambas potencias. En EEUU, la balanza entre libertad-seguridad se ha inclinado hacia la 'securitización' de un modo mucho más acusado que en la UE. Prueba de ello son las leyes que permiten las prácticas de vigilancia masiva que son inaceptables en el ordenamiento jurídico europeo (López Aguilar, 2017, p. 567).

Piñar Mañas (2005, p. 38) comparte el sentir europeo cuando opina que efectivamente es imprescindible adoptar medidas eficaces en la lucha contra el terrorismo, pero que esta tarea debe ser respetuosa con los derechos fundamentales, pues 'de lo contrario se estaría produciendo ya la primera y capital victoria de los terroristas: restringir el marco de libertades y derechos que, afortunadamente, caracterizan a las sociedades occidentales'. Reforzando esta postura, el TJUE volvió a pronunciarse a favor de la privacidad frente al acceso a los datos por motivos de seguridad en el ámbito intracomunitario en los casos La Quadrature du net y Privacy International.[93]

La otra gran diferencia entre las dos potencias está relacionada con la distinta concepción del derecho a la privacidad en el mercado. La protección en la UE como derecho fundamental impide la comercialización de los datos personales (Otero García Castrillón, 2022), mientras que en EEUU generaron un volumen de negocio de 76.000 millones de dólares en el año 2018 (Shapiro y Siddhartha, 2019, p. 3).

[93] En ambas sentencias, el TJUE concluyó que, a efectos de la protección de la seguridad nacional, la legislación nacional de los Estados Miembros, sólo excepcionalmente y de manera proporcional, puede permitir que los organismos públicos puedan requerir a los proveedores de servicios de comunicación electrónica el acceso a datos de tráfico y de localización de modo general e indiscriminado. Ver STJUE (Gran Sala) de 6 de octubre de 2020, en los asuntos La Quadrature du net y otros, asuntos C-511/18, C-512/18 y C-520/18 y STJUE (Gran Sala) de 6 de octubre de 2020 en los asuntos Privacy international c. Secretary of State for Foreign and Commonwealth Affairs y otros. C-623/17.

A diferencia de la UE, en EEUU la ley no proporciona garantías frente a las amenazas que plantea el sector privado a la privacidad (Cole y Fabbrini, 2015, p. 221) y prefiere dejar la regulación de los datos en manos de la autorregulación (Reidenberg, 1999, p. 771). Según su filosofía, con este sistema se protege la privacidad de forma eficiente sin intervención del gobierno, lo cual repercute favorablemente en el desarrollo de la tecnología. Se entiende que las propias empresas velarán por los datos para que los consumidores se sientan protegidos y confíen en ellas, y así mejorar sus beneficios comerciales (Reidenberg, 1999, p.774). W. Gregory Voss (2019, p. 435) considera que este sistema, propio de la ideología americana de '*laissez faire*',[94] pudiera estar promovido por el interés empresarial para dejar fuera del proceso a legisladores y a interesados. También critica la falta de rendición de cuentas al gobierno y la carencia de medios a través de los cuales los ciudadanos puedan reclamar sus derechos de forma eficaz.

En resumen, mientras EEUU considera que la protección de datos de la UE es una forma de proteccionismo comercial que perjudica la innovación tecnológica, la UE entiende que los derechos fundamentales de protección de datos no se pueden dejar desprotegidos en manos del mercado. Por lo tanto, como apuntan Schwartz y Peifer (2017, p. 157), 'los legisladores y los académicos de cada sistema ven al otro lado con dudas y, a veces, con incredulidad'. En el mismo sentido, Kuner (2017, p. 917) añade que el problema no es la falta de un acuerdo político sobre cómo regular las transferencias internacionales de datos, sino la falta de voluntad de la UE y los EEUU para considerar posiciones que van más allá de las asunciones subyacentes de sus propios sistemas.

2.2. ¿Un tercer acuerdo?

Tras Schrems II, el Departamento de Comercio de EEUU y la Comisión Europea anunciaron el inicio de un diálogo para estudiar la posibilidad de mejorar el acuerdo

[94] W. Gregory Voss identifica la política de *laissez-faire* y el neoliberalismo en los Estados Unidos (y el enfoque resultante en la autorregulación allí) como uno de los obstáculos para la harmonización de las políticas de privacidad de los datos entre EEUU y la UE. Ver Voss, W.G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. *Journal of Law, Technology & Policy, The University of Illinois*, pp.432-435.

invalidado de un modo que permita cumplir con la doctrina jurisprudencial (Comisión Europea, 2020).

Varios son los autores que ponen el foco de atención en el papel de la Comisión Europea a la hora de negociar un posible tercer acuerdo. Y es que, las sentencias Schrems I y II ya han puesto en evidencia dos veces la deficiente actuación de la Comisión al evaluar el nivel adecuado de EEUU, lo cual, Oreste Pollicino (2020) califica como 'perseverancia diabólica'. Por otro lado, Costello (2020, p. 1059) argumenta que unos meros cambios al Escudo de Privacidad, como antes se hizo con el Puerto Seguro, no sería una postura creíble ni sostenible. Además, en palabras del propio autor, dañaría la credibilidad de la independencia e integridad de la Comisión en la protección de los derechos de los ciudadanos en negociaciones internacionales (Costello, 2020, p. 1059).

Propp y Swire (2020) opinan que para alcanzar un marco jurídico estable para las transferencias de datos entre la UE y EEUU es preciso que se atienda a las preocupaciones del TJUE respecto a los derechos fundamentales recogidos en los artículos 7, 8 y 47 de la CDFUE. Recordemos que Schrems II identificó dos formas en las que los programas de vigilancia de EEUU llevados a cabo bajo la Sección 702 de la FISA y la EO 12333 carecen de una equivalencia sustancial con el derecho de protección de datos de la UE. La primera fue que esta normativa infringe el 'principio de proporcionalidad' y la segunda es que carece de medios para que los ciudadanos europeos puedan reclamar de forma 'eficaz y exigible' en caso ver vulnerados sus derechos (Propp y Swire, 2020). Por lo tanto, es preciso que la Comisión lleve a cabo esta vez una esmerada evaluación de EEUU y que introduzca los cambios necesarios para que una nueva decisión de adecuación sea capaz de resistir otro escrutinio del TJUE.

Kuner (2020) cree que sólo un cambio de la legislación estadounidense a la altura del alto listón marcado por el TJUE podría hacer posible la firma de un nuevo acuerdo transatlántico estable y viable. Sin embargo, la mayoría de la doctrina ve con escepticismo que EEUU lleve a cabo una reforma de su legislación sobre seguridad nacional (Kuner, 2020; Murphy, 2022; Chander, 2020; Propp y Swire, 2020).

Por otra parte, a la vista de Schrems II, no parece que el TJUE vaya a cambiar su línea de defensa de los derechos de privacidad y protección de datos por conveniencia

económica sino todo lo contrario (Murphy, 2021, p.3). En este sentido, Vardanyan y Stehlik (2020, p. 120) opinan que el objetivo de priorizar la protección de los derechos fundamentales no debe lograrse ignorando los factores económicos dado que eso podría volverse en contra de los propios derechos fundamentales. Otero García-Castrillón (2022) señala que el debate gira entre el proteccionismo y el liberalismo económicos y el reto es hallar el equilibrio entre la protección a la privacidad preservando los beneficios del comercio digital. Esta misma autora argumenta que una protección de datos demasiado estricta puede restringir en exceso el flujo de datos a terceros países mientras que, por el contrario, escasa protección 'puede afectar a los derechos fundamentales de los individuos y a la confianza de los consumidores, perjudicando igualmente el comercio internacional'.

Algunos autores critican al TJUE por haber elevado demasiado el estándar de protección de datos requerido por la UE para permitir las transferencias internacionales a terceros países de modo que puede ocurrir que sea prácticamente imposible alcanzarlo (Costello, 2020; Kuner 2020).[95]

Todo esto parece indicar que nos encontramos ante un escenario en el que ninguna de las dos partes está dispuesta a ceder fácilmente. El Escudo de Privacidad se firmó sólo unos meses después de la invalidación de su predecesor, sin embargo, esta vez las negociaciones se están alargando. A mediados de 2021, ambas partes manifestaron el compromiso compartido para encontrar un sucesor integral del Escudo de Privacidad que esté totalmente en línea con los requisitos de *Schrems II* y con la ley de EEUU, pero desde la UE se destacó que la velocidad no debe prevalecer sobre la calidad y que hay que evitar un Schrems III (Propp, 2021).

La reciente reunión en Bruselas entre el presidente de EEUU, Joe Biden, y la presidenta de la Comisión Europea, Úrsula von der Leyen, parece que acelerará el proceso de obtener un tercer acuerdo. El presidente estadounidense prometió 'un acuerdo sin precedentes' sobre la protección de la privacidad de los datos y la seguridad de los ciudadanos, a lo que von der Leyen añadió que 'permitirá el flujo de datos entre la UE y EEUU de forma predecible y fiable, equilibrando la seguridad, el derecho a la

[95] Kuner (2020) incluso sostiene que Schrems II puede afectar negativamente a la influencia de la normativa europea de protección de datos en el mundo. Este autor opina que Schrems II puede hacer que algunos países se pregunten si vale la pena esforzarse por alcanzar los estándares de protección de datos de la UE y entablar relaciones tan largas si al final pueden acabar invalidadas. También cree que puede hacer que el modelo del RGPD sea un modelo menos atractivo para terceros países. https://verfassungsblog.de/schrems-ii-re-examined/.

privacidad y la protección de datos' (Expansión, 2022). No obstante, en el momento en el que se escribe el presente trabajo, esta promesa se trata de un mero anuncio político, no de un texto que pueda ser analizado.

Aun así, gracias a un Comunicado de la Casa Blanca, hemos podido conocer algunos detalles. EEUU se ha comprometido a implementar nuevas salvaguardias para superar los dos principales escollos señalados por el TJUE. Por un lado, el nuevo marco jurídico asegura que la recopilación de datos personales se llevará a cabo de forma proporcionada y sólo cuando sea necesario para cumplir objetivos legítimos de seguridad nacional. En este sentido, las agencias de inteligencia deben garantizar la supervisión de los estándares de privacidad y libertades civiles. Por otro lado, se creará un nuevo sistema de reparación individual en varios niveles, que incluye un Tribunal de Revisión de Protección de Datos independiente. Este Tribunal estaría formado por miembros ajenos al gobierno de EEUU con plena autoridad para resolver los recursos de los ciudadanos europeos e imponer medidas correctoras cuando fuese necesario (The White House, 2022).

2.3. La doctrina opina

Es extensa la literatura académica que se ha desarrollado con el fin de aportar soluciones a la cuestión de las transferencias internacionales de datos entre la UE y EEUU.

Ante el fracaso de los dos Acuerdos y la incertidumbre que provocó Schrems II, muchos autores propusieron la localización de datos dentro de la UE. Esto es, que los datos sean almacenados y tratados en servidores ubicados dentro de las fronteras de los Estados Miembros. Su argumento es que, de este modo, los datos quedan fuera del alcance de los servicios de inteligencia extranjeros y se facilita a los ciudadanos europeos el derecho a hacer valer sus derechos de protección de datos (Kuner, 2017, p. 913).

Sin embargo, en opinión de Chander (2020, pp. 8-14), la localización de datos no es una buena opción. Este autor argumenta que de las revelaciones de Snowden se deduce que no se puede garantizar que EEUU no pueda acceder a los datos aún dentro

de la UE. Por otro lado, aunque se almacenen los datos a este lado del Atlántico, siempre va a ser necesario realizar transferencias internacionales a EEUU en el contexto tanto de relaciones comerciales como de redes sociales, etc. Además, la naturaleza propia de Internet provoca que incluso las transferencias entre dos Estados Miembros puedan enrutarse a través de EEUU. Por lo tanto, Chander opina que la localización de datos es costosa, va en contra del espíritu del RGPD de promover el flujo de datos internacionales para el desarrollo del comercio internacional y, por último, puede perjudicar las labores de ciberseguridad.

Otra corriente de pensamiento considera que la mejor solución sería que EEUU adoptase una ley federal de protección de datos. Andraya Flor (2022, pp. 2041-2055) comparte esta postura y considera que éste es el momento oportuno para hacerlo por dos razones. La primera de ellas está relacionada con su propio interés interno. Así, en 2018 el Estado de California dictó la *California Consumer Privacy Act,* convirtiéndose en la primera norma estadounidense inspirada en el RGPD. Desde entonces y hasta ahora, otros veintisiete Estados promulgaron sus propias leyes de seguridad. Por esta razón, EEUU debería aprovechar la ocasión para dictar una norma de alcance federal con el fin de armonizar su política interna y evitar discrepancias que puedan dificultar las relaciones comerciales entre sus propios Estados. La segunda razón es que, a la vista de Schrems II y la postura adoptada por Europa, una norma así facilitaría un acuerdo transatlántico estable y duradero.[96] Solove y Schwartz (2019) confían en que es posible realizar un enfoque integral de la protección datos que acabe con las diferencias entre ambas potencias a partir de los '*Principles of Law, Data Privacy'* creados por el American Law Institute. Estos principios fueron elaborados con el fin de servir de guía para todos aquellos actores, tanto públicos como privados, que puedan tener relación con la privacidad.

Desde otra óptica distinta pero relacionada con el gran escollo para alcanzar un entendimiento, Cole y Fabbrini (2016) proponen un pacto transatlántico basado en el compromiso de no espiar a los nacionales de la otra parte dentro de sus propias fronteras, como es el caso del acuerdo de no espionaje entre EEUU y Reino Unido. En un proyecto todavía más ambicioso, Martínez Martínez (2020) considera urgente la adopción de un marco internacional de privacidad y recuerda que, ya en el año 2011, la

[96] Para saber más sobre los Estados de EEUU que han adoptado normas de protección de datos, se recomienda consultar el siguiente enlace a la página web de la 'International Association of Privacy Professionals' https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

31ª Conferencia Internacional de Autoridades de Protección de Datos advirtió de la necesidad de reconocer los derechos a la protección de datos y a la privacidad 'en un instrumento legislativo universal y vinculante'.[97]

No obstante, aunque estas aportaciones podrían considerarse posibles soluciones a largo plazo, para un futuro más cercano, tal vez sea más adecuada la postura de Propp y Swire (2020). Estos autores sugieren que EEUU debe crear un sistema de investigación administrativa y de revisión judicial que responda a las denuncias de los ciudadanos europeos contra el gobierno por posibles abusos en las labores de vigilancia. Propp y Swire afirman que la Ley de Vigilancia de EEUU ya cuenta con mecanismos institucionales que permiten llevar a cabo estos cambios sin necesidad de realizar grandes modificaciones legislativas. Por su parte, Murillo de la Cueva (2020) apunta a un acuerdo en el que quepa la posibilidad de discriminar en función de la naturaleza de los datos afectados. También propone la posibilidad de responsabilizar al destinatario en caso de accesos indebidos a los datos objeto de la transferencia con la consecuente obligación de compensar al perjudicado.

V. CONCLUSIONES

PRIMERA- Las sentencias Schrems I y II han demostrado que EEUU es incapaz de garantizar un nivel de protección de datos personales sustancialmente equivalente al de la UE.

Como se ha plasmado en el análisis de ambas sentencias, el TJUE demostró que, bajo el paraguas del artículo 702 del FISA y la EO 12333, las autoridades públicas americanas no cuentan con límites para desarrollar los programas de vigilancia con fines de inteligencia. Esto implica la violación de los derechos de privacidad y de protección

[97] Es posible acceder a la Resolución sobre estándares internacionales de privacidad de la citada Conferencia Internacional de Autoridades de Protección de Datos en el siguiente enlace https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwih65eN5ev2AhUIgc4BHaeaCR8QFnoECAQQAQ&url=https%3A%2F%2Fedps.europa.eu%2Fsites%2Fedp%2Ffiles%2Fpublication%2F09-11-05_madrid_int_standards_es.pdf&usg=AOvVaw1-meMgX6JoEj9vtwtqwt-m

de datos reconocidos en los artículos 7 y 8 de la CDFUE, respectivamente. Además, ni estas normas ni la figura del Defensor del Pueblo garantizan medios efectivos para que los ciudadanos europeos puedan alegar una vulneración de estos derechos fundamentales, lo cual viola el artículo 47 de la CDFUE.

Así pues, queda demostrado que la normativa estadounidense no permite calificar su nivel de protección de datos como adecuado conforme al artículo 45 del RGPD. La opinión de esta autora coincide con la de la doctrina cuando argumenta que, mientras que EEUU no lleve a cabo una reforma de su legislación de seguridad nacional, no se podrá alcanzar un acuerdo estable y capaz de soportar un escrutinio del TJUE.

SEGUNDA- Ambas sentencias ponen de manifiesto la firme postura del TJUE como defensor de los derechos de privacidad y de protección de datos frente a las actuaciones de los poderes públicos en el ejercicio de acciones de seguridad nacional.

Con estas sentencias, el TJUE consolida su jurisprudencia en defensa de estos derechos fundamentales frente a las actuaciones de vigilancia masiva faltas de proporcionalidad.

Las diferentes posturas adoptadas por la UE y EEUU respecto a los límites de las acciones en pro de la seguridad nacional son un escollo para las transferencias internacionales de datos. Esta diferencia parte de la distinta concepción del derecho de privacidad. En Europa, preocupados por la dignidad y el honor, se ha catalogado el derecho a la privacidad y al derecho a la protección de datos personales como fundamentales. En EEUU, preocupados por la libertad e inmersos en la filosofía del *laissez faire,* los consideran como derechos del consumidor.

Al juicio de esta autora, EEUU debería realizar el esfuerzo de considerar la posibilidad de ofrecer a sus ciudadanos una protección similar a la ofrecida en la UE. Le convendría aprovechar el impulso iniciado por algunos de sus Estados y promover una ley federal de protección de datos. Al tener un estándar similar al de la UE, ello facilitaría enormemente la relación transatlántica.

TERCERA- La Comisión Europea no actuó con diligencia en ninguna de las dos decisiones de adecuación adoptadas con EEUU.

Las razones que invalidaron el Escudo de Privacidad fueron básicamente las mismas que llevaron a la invalidación del Puerto Seguro. El TJUE constató en ambas ocasiones que la Comisión no había realizado diligentemente la evaluación del nivel de protección de EEUU y que no se reconocía a los ciudadanos europeos el derecho a una tutela judicial efectiva. Además, los cambios introducidos en el Escudo de Privacidad respecto al Acuerdo anterior resultaron insuficientes.

Coincido con la doctrina en que unas meras modificaciones en el Escudo de Privacidad no serían suficientes para obtener un nuevo acuerdo sólido. La Comisión debería tener en cuenta las críticas del Parlamento y del CEPD antes de volver a adoptar una nueva decisión de adecuación.

CUARTA- La Sentencia Schrems II tiene consecuencias más allá de la relación con EEUU. La doctrina resultante de esta sentencia tiene implicaciones significativas en el régimen jurídico de las transferencias internacionales.

Si Schrems I tuvo consecuencias en la regulación de las decisiones de adecuación, Schrems II va a cambiar el régimen de transferencias internacionales de datos basadas en las garantías del artículo 46 del RGPD. El TJUE reinterpreta el capítulo V del RGPD para exigir el mismo nivel de protección de datos a todas las transferencias internacionales, independientemente del instrumento jurídico que se utilice.

Como ya se expuso en el presente trabajo, en teoría, este novedoso sistema parece atractivo al acabar con la ‘ficción legal’ que suponían las cláusulas tipo. No obstante, en la práctica, genera mucha incertidumbre en la gestión de las transferencias de datos a EEUU y al resto del mundo. A mi juicio, la UE debería dictar una nueva legislación que recoja y aclare la doctrina de Schrems II adaptándose de nuevo a la cambiante realidad tecnológica.

QUINTA- La importancia económica de la relación transatlántica requiere que ambas partes se involucren en un tercer intento de adoptar una decisión de adecuación que vuelva a permitir el tráfico fluido de datos personales.

Tras la invalidación del Escudo de Privacidad, EEUU se ha convertido en un tercer país que carece de nivel de protección adecuado, por lo que las transferencias internacionales de datos se realizarán basándose en las garantías del artículo 46 del RGPD o en alguna de las excepciones de su artículo 49.

Esto ha afectado negativamente en la importante relación económica que existe entre ambas potencias. Recordemos que la mayoría de las grandes tecnológicas que ofrecen servicios a las empresas europeas tienen su sede en EEUU, por lo que cualquier transferencia entre Estados dentro de la Unión puede acabar en EEUU, convirtiéndose en una transferencia ilegal. Esta situación crea una inseguridad jurídica que, bien puede dificultar la gestión de los datos con el consecuente coste económico, o bien puede resultar en una imposibilidad de realizar la transferencia.

Gran parte de la doctrina considera que el TJUE ha elevado el estándar de protección de datos personales de un modo que puede ser difícil de alcanzar. Bajo el punto de vista de esta autora, la UE debería buscar un equilibrio entre privacidad y seguridad, así como entre privacidad y desarrollo económico. Vivimos en un mundo globalizado bajo el imperio de Internet, donde cada vez más las relaciones comerciales se llevarán a cabo de forma digital. Elevar los requisitos para realizar las transferencias internacionales podría llevarnos a perder competitividad y alejarnos de establecer relaciones comerciales con terceros países, lo cual resultaría en un perjuicio para todos los ciudadanos europeos.

SEXTA- Tras casi dos años desde la invalidación del Escudo de Privacidad, EEUU y la UE han anunciado un acuerdo político que debe materializarse en una decisión de adecuación. EEUU se ha comprometido a corregir los dos principales escollos para alcanzar una evaluación favorable de la Comisión sobre su nivel de protección de datos. Posibilidad de un tercer acuerdo o de un 'tercer Schrems'.

Como se ha visto en este trabajo, las dos sentencias Schrems no han hecho más que poner en evidencia la reafirmación de la UE y EEUU en sus posturas respecto a la privacidad. Por ello, la mayoría de la doctrina no confía en que EEUU realice grandes cambios en su política de inteligencia. Sobre todo, cuando la UE se muestra cada vez más preocupada por defender los derechos de sus ciudadanos aunque ello implique un perjuicio para la relación transatlántica.

Sólo el futuro determinará si esta vez los compromisos estadounidenses están a la altura de las expectativas europeas y si la Comisión será capaz de realizar diligentemente su trabajo. No sólo está en juego un importante acuerdo, sino también el prestigio y la credibilidad de la UE como abanderada de la promoción del derecho a la protección de datos a nivel mundial.

Tal vez el acercamiento entre las dos potencias como respuesta a la reciente invasión rusa en Ucrania haya conseguido acelerar un proceso de negociación que llevaba demasiado tiempo estancado. Esperemos que la Comisión tenga en cuenta las críticas a las que el proyecto se ha enfrentado para redactar un marco jurídico sin fisuras y flexible a correcciones posteriores para así evitar llegar de nuevo a los tribunales.

REFERENCIAS

LEGISLACIÓN

EU

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DOUE 4 de mayo de 2016).

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE 23 de noviembre de 1995).

EEUU

Executive Order 12333. United States Intelligence Activities (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)).

Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-11 et sq. (1978).

JURISPRUDENCIA

STJUE (Gran Sala), de 6 de noviembre de 2003, asunto C-101/01, Göta hovrät (Suecia) c. Lindqvist, apartado 71.

STJUE (Gran Sala), de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland c. Ministerio de Comunicaciones, Marina y otros.

STJUE (Gran Sala), de 13 de mayo de 2014, asunto C 131/12, Google Spain, S.L., Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González.

STJUE (Gran Sala) de 6 de octubre de 2015, asunto C-362/14, Maximillian Schrems contra Data Protection Commissioner.

STJUE (Gran Sala), de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB contra Post- och telestyrelsen y Secretary of State for the Home Department contra Tom Watson y otros.

STJUE (Gran Sala) de 16 de julio de 2020, asunto C-311/18 Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems.

STJUE (Gran Sala) de 6 de octubre de 2020, en los asuntos La Quadrature du net y otros, asuntos C-511/18, C-512/18 C-520/18

STJUE (Gran Sala) de 6 de octubre de 2020, en los asuntos Privacy international c. Secretary of State for Foreign and Commonwealth Affairs y otros. C-623/17.

STJUE (Gran Sala) de 16 de julio de 2020, asunto C-311/18 Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems.

OBRAS DOCTRINALES

Álvarez Caro, M. & Recio Gayo, M. (2015). Hacia un acuerdo Safe Harbour renovado para la transferencia internacional de datos entre EE.UU y la UE. *Instituto de Derecho Europeo e Integración Regional*, 25, 1-26.

Bignami, F. (2020/7/29). Schrems II: The Right to Privacy and the New Illiberalism. *VerfassungBlog*. https://verfassungsblog.de/schrems-ii-the-right-to-privacy-and-the-new-illiberalism.

Blasi Casagran, C. (2017). ¿Es compatible con la normativa europea de protección de datos? *Revista General de Derecho Europeo*, 42, 193-217.

Bracero, F. (9 de febrero de 2022). *Facebook dice ahora que 'en absoluto' ha amenazado con dejar Europa.* La Vanguardia. https://www.lavanguardia.com/tecnologia/20220209/8046185/facebook-dice-absoluto-amenazado-dejar-europa.html.

Castellanos Rodríguez, A. (2017). El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio *Privacy Shield*. *Institut de Ciències Polítiques i Socials*, 350, 1-34.

Chander, A. (2020). Is Data Localization a Solution for Schrems II? *Journal of International Economic Law*, 23(3), pp. 771–784.

Christakis, T. (2020). After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe. *European Law Blog.* https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe.

Cole, D. & Fabbrini, F. (2016). Bridging the Transatlantic Divide? The European Union, the United States and the Protection of Privacy Across Borders. *International Journal of Constitutional Law*, 14, (1), 220-237.

Cordero Álvarez, C. I. (2019). La transferencia internacional de datos con terceros Estados en el nuevo Reglamento europeo: Especial referencia al caso estadounidense y la Cloud Act. *Revista Española De Derecho Europeo, (70)*, 49.108.http://www.revistasmarcialpons.es/revistaespanoladerechoeuropeo/article/view/54.

— (2022). Transferencia de datos personales fuera del EEE en el nuevo marco del reglamento general: especial referencia al caso estadounidense y el Reino Unido tras el Brexit. En E. Rodríguez Pineu y E. Torralba Mendiola (Ed.), *La protección de las transmisiones de datos transfronterizas*. Editorial Aranzadi.

Costello, R. A. (2020). Schrems II: Everything Is Illuminated? *European Papers* 5, 1045-1059. https://www.europeanpapers.eu/en/europeanforum/schrems-II-everything-is-illuminated.

Fahey, E., & Terpan, F. (2021). Torn Between Institutionalisation & Judicialisation: The Demise of the EU-US Privacy Shield. *Indiana Journal of Global Legal Studies*, 28(2), 205–244.

Flor, A. (2021). The impact of Schrems II: next steps for U.S. data privacy law. *The Notre Dame Law Review*, 96, (5), 2025-2058.

Fuentes Máiquez, A. (2021). Comentario de la STJUE de 16 de Julio de 2020, C-311/18 (Schrems II). *Icade. Revista De La Facultad De Derecho*, 110, 1-10.

Gonzalo Domenech, J.J. (2019). 'Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de

control aplicados por los Estados Miembros'. *Cuadernos de Derecho Transnacional*, 1, 350-371.

Kenneth, P. & Swire, P. (2020). Geopolitical Implications of the European Court's Schrems II Decision. *Lawfare*. https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision.

Kuner, C. (2017). Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, 18(4), 881-918.

–(2019). The Internet and the Global Reach of EU Law. En M. Cremona y J. Scott (Ed.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*. Oxford University Press.

–(2020). Schrems II Re-Examined. *Verfassungsblog.* https://verfassungsblog.de/schrems-ii-re-examined, DOI: 10.17176/20200825-183419-0.

López Aguilar, J. F. (2017). La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU. *Teoría y Realidad Constitucional,* 39, pp. 557–581.

Lynskey, O. (2020). Delivering Data Protection: The Next Chapter. *German Law Journal.* 21, 80-84.

Maldonado, E. (2020). Bridging the gap in transatlantic data protection, Discussion Paper, No. 4/20. *Europa-Kolleg Hamburg, Institute for European Integration*, 1-24.

Martínez Martínez, R. (2020). Schrems II. Una breve reflexión desde los derechos fundamentales. *La Ley Privacidad*, 5.

Murillo de la Cueva, P. L. (2020). Entrevista: El perpetuum mobile del derecho a la protección de datos: no solo mantenerlo, sino reforzarlo. *La Ley Privacidad.*

Murphy, M. (2022). Assessing the implications of Schrems II for EU-US data flow. *International and Comparative Law Quarterly*, 71 (1), 245-262.

Ortega Giménez, A. & García Escobar, E. (2020). Transferencias internacionales de datos personales UE-EE.UU., tras la STJUE 'SCHREMS II'. *Revista Lex Mercatoria*, (16), 2, 7-15.

Otero García-Castrillón, C. (2022). Protección de datos en la economía digital. Una aproximación desde la regulación del comercio internacional. En E. Rodríguez Pineu y E. Torralba Mendiola (Ed.), *La protección de las transmisiones de datos transfronterizas*. Editorial Aranzadi.

Peers, S. (2015). When super-regulators fight: the 'one-stop shop' in the proposed Data Protection Regulation, *EU Law Analysis blog*. http://eulawanalysis.blogspot.com.es/2015/03/when-super-regulators-fight-one-stop.html.

Pérez, E. (6 de mayo de 2021*). Microsoft dejará de enviar datos personales a los EE.UU y los guardará en servidores europeos: los primeros en adaptarse tras el 'Privacy Shield'*. Xataka. https://www.xataka.com/privacidad/microsoft-dejara-enviar-datos-personales-a-ee-uu-guardara-servidores-europeos-para-ser-primeros-adaptarse-privacy-shield.

Piñar Mañas, J.L. (2005). El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro. *Asamblea: revista parlamentaria de la Asamblea de Madrid*, 13, 21-46.

–(2016). 'Transferencias de datos personales a terceros países u organizaciones internacionales', Álvarez Caro, M. y Recio Gayo, M. (Coord.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (1ª ed., 427-460). Reus Editorial.

Pollicino, O. (2020). Diabolical Persistence. Thoughts on the Schrems II Decision. *Media Laws.* https://www.medialaws.eu/rivista/diabolical-persistence-thoughts-on-the-schrems-ii-decision/.

Polo Roca, A. (2021). Las transferencias internacionales de datos: regulación actual y su incidencia en las relaciones exteriores de la unión europea. *Revista Aragonesa de Administración Pública,* 57, 325-369.

Propp, K. & Swire, P. (2020). After Schrems II: A Proposal to Meet the Individual Redress Challenge. *Georgia Tech Scheller College of Business Research Paper* (No. 3680148). http://dx.doi.org/10.2139/ssrn.3680148.

Propp, K. (2021). Progress on Transatlantic Data Transfers? The Picture After the US-EU Summit. *Lawfare*. https://www.lawfareblog.com/progress-transatlantic-data-transfers-picture-after-us-eu-summit.

Puerto, M.I. & Sferrazza, P. (2017). La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional. *Revista Derecho del Estado*. 40 (dic. 2017), 209-236.

Recio Gayo, M. (2019). Nivel adecuado para transferencias internacionales de datos. *Derecho PUCP: Revista de la Facultad de Derecho*, 83, 207-240.

Reidenberg, J. R. (1999). Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford Law Review*, *52*(1315 (1999–2000). https://ir.lawnet.fordham.edu/faculty_scholarship/41/.

Rodríguez Ayuso, J. F. (2021). Alternativas de las Administraciones Públicas en materia de intercambios de información UE-EEUU. *Revista Aragonesa de Administración Pública*, 56, 342-367.

Ruiz Tarrías, S. (2021). La Sentencia del Tribunal de Justicia de la Unión Europea en el asunto Schrems II o cómo los datos personales pueden terminar viajando sin equipaje. *Revista Española De Derecho Europeo*, (76), 111-162.

Schwartz, P. M. & Peifer K. N. (2017). Transatlantic Data Privacy Law. *The Georgetown Law Journal*, 106 (115), pp. 115-179.

Shapiro, R. and Siddhartha, A. (2019). Who Owns Americans' Personal Information and What Is It Worth? *Future Majority*, 1-22.

Sobrino García, I. (2021). Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Estados Unidos. *Revista de Derecho Comunitario Europeo*, 68, 227-256. https://recyt.fecyt.es/index.php/RDCE/article/view/82707.

Solove, D. J. and Schwartz, P. M. (2019). ALI Data Privacy: Overview and Black Letter Text. GWU Law School Public Law Research Paper No. 2019-67, 1-47.

Terpan, F. (2018). EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One? *European Papers*, 3, 1045-1059.

Uría Gavilán, E. (2016). 'Derechos fundamentales *versus* vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de

2015 en el asunto C-362/14 Schrems'. *Revista de Derecho Comunitario Europeo*, 53, 261-282.

Vardanyan, L., y Stehlík, V. (2020). Schrems II: will it really increase the level of privacy protection against mass surveillance? *Bratislava Law Review*, 4(2), 111-128.

Voss, W. G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. *Journal of Law, Technology & Policy, The University of Illinois*, pp. 405-463.

Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity Versus Liberty. *The Yale Law Journal*, 113, pp. 1153-1219.

INFORMES Y OTROS DOCUMENTOS

Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa (2018). *Manual de legislación europea en materia de protección de datos.* Luxemburgo: Oficina de Publicaciones de la Unión Europea.

Comisión Europea (2017, 15 febrero). Comunicación de la Comisión al Parlamento europeo y al Consejo: Intercambio y protección de los datos personales en un mundo globalizado. COM (2017) 7 final/2, 15 de febrero de 2017. https://ec.europa.eu/transparency/regdoc/rep/1/2017/ES/COM-2017-7-F2-ES-MAIN-PART-1.PDF.

–(2020, 10 agosto). Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross. https://ec.europa.eu/newsroom/just/items/684836.

Congressional Research Service (2021, 22 septiembre). *U.S.-EU Privacy Shield and Transatlantic Data Flows.* CRS Report, 1-24. https://crsreports.congress.gov/product/pdf/R/R46917.

Economist & Jurist. (2022, 7 febrero). *Los organismos de protección de datos cercan a Google Analytics.* https://www.economistjurist.es/articulos-juridicos-destacados/derecho-comunitario/los-organismos-de-proteccion-de-datos-cercan-a-google-analytics/.

European Centre for International Political Economy and Kearney Global Business Policy Council (2021, 30 junio). ‘The Economic Costs of Restricting the Cross-border Flow of Data’, https://www.wita.org/atp-research/cross-border-data-restrictions/.

Expansión. (2022, 25 marzo). La UE y EEUU llegan a un acuerdo transferir datos personales garantizando la privacidad. *EXPANSIÓN*. https://www.expansion.com/juridico/actualidad-tendencias/2022/03/25/623da4b9468aeb816d8b4616.html.

The White House. (2022, 25 marzo). FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework. https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.