LAS DECISIONES DE ADECUACIÓN EN LAS TRANSFERENCIAS INTERNACIONALES DE DATOS. EL CASO DEL FLUJO DE DATOS ENTRE LA UNIÓN EUROPEA Y ESTADOS UNIDOS

ITZIAR SOBRINO GARCÍA[1]
isobrino@uvigo.es

Cómo citar/Citation
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.
doi: https://doi.org/10.18042/cepc/rdce.68.07

Resumen

Este trabajo tiene como objetivo analizar los elementos que han llevado a la invalidación del actual *Privacy Shield,* el acuerdo entre la Unión Europea y Estados Unidos para las transferencias transfronterizas de datos, como consecuencia de la sentencia *Schrems II*. Para ello, este artículo se enfoca en establecer el concepto de nivel adecuado y decisión de adecuación a través del análisis legal y revisión de la literatura. Una vez estudiados, se examinan tras una breve contextualización del acuerdo que lo precedió, las lagunas o problemas iniciales del *Privacy Shield*, así como la argumentación dada por el Tribunal de Justicia de la Unión Europea para su invalidación.

Palabras clave

Protección de datos; transferencias internacionales; nivel de adecuación EE. UU.; UE; RGPD; caso *Schrems II*; TJUE.

[1] Investigadora contratada predoctoral de la Xunta del Área de Derecho Administrativo de la Universidad de Vigo.

THE ADEQUACY DECISIONS IN CROSS-BORDER DATA TRANSFERS. THE CASE OF DATA FLOW BETWEEN THE EUROPEAN UNION AND THE UNITED STATES

Abstract

This paper aims to analyze the elements that have led to the invalidation of the current Privacy Shield, the agreement between the European Union and the United States for cross-border data transfers, because of the *Schrems II* case. To this end, this work focuses on establishing the concept of adequate level and adequacy decision through legal analysis and literature review. Once studied, after a brief contextualization of the agreement that preceded it, the gaps or initial problems of the Privacy Shield are examined, as well as the arguments given by the Court of Justice of the European Union for its invalidation.

Keywords

Data protection; cross-border data transfer; adequate level; U.S.; EU; GDPR; Schrems II case; CJEU.

LES DÉCISIONS D'ADÉQUATION DANS LES TRANSFERTS INTERNATIONAUX DE DONNÉES. LE CAS DES FLUX DE DONNÉES ENTRE L'UNION EUROPÉENNE ET LES ÉTATS-UNIS

Résumé

Ce travail vise à analyser les éléments qui ont conduit à l'invalidation du bouclier de protection des données actuel, l'accord entre l'Union européenne et les États-Unis pour les transferts de données transfrontaliers, à la suite de l'arrêt *Schrems II*. À cette fin, cet article se concentre sur l'établissement du concept de niveau adéquat et de décision d'adéquation au moyen d'une analyse juridique et d'une revue de la littérature. Une fois étudiés, après une brève contextualisation de l'accord qui l'a précédé, les lacunes ou problèmes initiaux du bouclier de protection des données sont examinés, ainsi que les arguments avancés par la Cour de justice de l'Union européenne pour son invalidation.

Mots clés

Protection de données les transferts internationaux; niveau d'adéquation; EUA; EU; RGPD; affaire *Schrems II*; CJUE.

SUMARIO

I. INTRODUCCIÓN

La era digital actual presenta un panorama económico y social cambiante, debido a la creación de productos y servicios que impulsan nuevas formas de relacionarse y comunicarse. Estos avances han dado lugar a medios que permiten la gestión automatizada de la información, generando como consecuencia que el análisis y recogida de cantidades ingentes de datos personales sea posible (Birnhack, 2008:508). Ha habido un crecimiento en la complejidad y el volumen del flujo de datos global, lo que ha provocado que los datos de carácter personal se hayan convertido en una parte esencial de la economía mundial (Schwartz, 2009:60). El mundo actual ya no se encuentra definido por fronteras o barreras físicas y las transferencias internacionales de datos han conllevado un crecimiento económico con un gran impacto positivo en todo el mundo (Bennett y Raab, 2003:257).

Con el tiempo, se hizo patente que para que las transacciones fueran factibles y pudieran garantizarse los diferentes derechos como el acceso a la información pública, las transferencias internacionales de datos debían ser objeto de una cooperación, alejada de aproximaciones unilaterales.

Sin embargo, estos factores han aumentado los riesgos en la privacidad de los ciudadanos, sobre todo en lo relativo a las transferencias de datos con terceros países, ya que estos pueden no ofrecer el mismo nivel normativo de

protección. No obstante, el legislador europeo ha sido consciente de que el bloqueo de los datos personales hacia el exterior no era la opción más acertada, ya que las economías actuales dependen en gran medida de la transmisión de datos personales hacia terceros países (Sobrino García, 2021: 29). El no evitar dicho bloqueo supondría la asfixia de sectores económicos tales como el comercio electrónico, los servicios financieros, el movimiento de personas entre países o el auxilio judicial internacional, que son parte integral de la economía actual globalizada (Moslemzadeh Tehrani *et al.*, 2018: 583).

Este panorama, unido a la relevancia que la Unión Europea (UE) ha otorgado a la protección de datos personales debido a su naturaleza de derecho fundamental, en un primer momento como parte integrante del derecho a la intimidad recogido en el art. 8 del Convenio Europeo de Derechos Humanos (CEDH)[2], y posteriormente como derecho fundamental independiente, como se reconoce en el Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[3] (en adelante Convenio 108), se ha ido traduciendo a lo largo de los años en una normativa comunitaria, incluyendo las transferencias internacionales como una parte clave, ya que esta regulación resulta vital para evitar la creación de oasis de datos (Wagner, 2018: 318).

Con carácter general, la normativa de la UE prohíbe el flujo de datos de sus ciudadanos fuera de sus fronteras, a menos que se transfieran a un tercer país u organización que cuente con un nivel adecuado de protección de datos. Esta restricción fue establecida en primer lugar, en 1995, por la Directiva 95/46/CE, 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[4] (en adelante Directiva 95/46) y posteriormente por el Reglamento (UE) 2016/679 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[5] (en adelante RGPD), que la reemplazó a su entrada en vigor en 2018. Sin embargo, ni la directiva anterior y ni el actual RGPD han establecido qué debe entenderse por nivel adecuado de protección de datos, quedando en manos de la jurisprudencia del Tribunal de Justicia de la UE y de diversos documentos oficiales.

A pesar de la existencia de normativa de la UE, las diferentes políticas implementadas por los países que pudieran afectar a los datos personales de

2 BOE 243, de 10 de octubre de 1979.
3 BOE 274, de 15 de noviembre de 1985.
4 DO L 281, de 24 de octubre de 1995.
5 DO L 119, de 27 de abril de 2016.

los ciudadanos generaron dudas y tensiones en el panorama europeo (Piñar Mañas, 2016: 440). El caso que se ha presentado como el más conflictivo y representativo a lo largo de los años es el de Estados Unidos (en adelante, EE.UU.).

La cantidad de datos que se transfieren entre la UE y EE.UU. resulta significativa, debido a que las inversiones de estas potencias son el verdadero motor de la relación transatlántica y definen en gran medida la forma de la economía global. En sus respectivas economías, los flujos internacionales de información personal representan un componente de comercio con un rápido alto crecimiento (Schwartz y Peifer, 2017: 119). En este sentido, las recientes estadísticas publicadas en la página web de la Comisión Europea revelaron que la relación económica entre la UE y EE.UU. supuso en cuanto a bienes 232 billones de euros en importaciones europeas y 384,4 billones de euros en exportaciones europeas, mientras que en atención a los servicios, 196,2 billones de euros en importaciones europeas y 179,4 billones de euros en exportaciones europeas durante el 2019[6]. Actualmente, la mayor parte del comercio implica el tratamiento de los datos personales de los ciudadanos europeos, puesto que numerosas compañías dependen del acceso a dichos datos para proporcionar sus servicios.

Aunque ambos reconocen que la privacidad de los datos personales es digna de protección, desde EE.UU. ha habido voces que han considerado la legislación europea demasiado proteccionista (Bender, 2016: 117), mientras que desde la UE siempre ha existido el debate sobre si las leyes norteamericanas han protegido suficientemente los datos personales de los ciudadanos europeos cuando las autoridades públicas estadounidenses los recopilan y procesan (Sobrino García, 2019: 689). Demasiada protección puede restringir de forma excesiva el comercio internacional, pero al mismo tiempo una escasa protección podría perjudicar los derechos fundamentales de los individuos, de ahí la necesidad de un equilibrio entre el flujo internacional de datos personales y su protección (Otero García-Castrillón, 2020).

Por ello, para mantener la estabilidad y el crecimiento económico entre la UE y EE.UU. elaboraron a finales de los noventa un acuerdo que permitiría las transferencias internacionales de datos entre ambos, bajo el nombre de *Safe Harbor* o Puerto Seguro[7]. No obstante, este acuerdo sufrió un duro

---

6 Véase la posición de la UE en el comercio a nivel mundial, disponible en: https://bit.ly/3rH76v9.

7 Decisión de la Comisión, 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 de puerto seguro para la protección de la vida privada y las

revés en 2013 tras las declaraciones de Edward Snowden sobre los programas de vigilancia norteamericanos y las prácticas de la National Security Agency[8]. Estas revelaciones demostraron a la UE que los datos de los ciudadanos europeos no gozaban de una protección adecuada y resultó en la invalidación del acuerdo en 2015 por el Tribunal de Justicia de la Unión Europea (en adelante TJUE) en su sentencia *Schrems I*[9]. Este panorama aumentó la inseguridad jurídica en el ámbito económico, lo que unido a la invalidación del *Safe Harbour* propició nuevas negociaciones para la creación de un nuevo acuerdo en 2016, *Privacy Shield* o Escudo de Privacidad.[10] Sin embargo, este último acuerdo ha sido también invalidado recientemente ya que el TJUE, en su sentencia *Schrems II*[11], sigue entendiendo que las exigencias de seguridad nacional de EE.UU. prevalecen sobre el marco legal de transferencias internacionales con la UE de manera intrusiva.

En este contexto y explorando dicha problemática, esta investigación analizará los elementos que llevaron a la invalidación del *Privacy Shield* tras la sentencia del caso *Schrems II*. En las páginas que siguen se contextualizará brevemente y en un primer momento la regulación de las transferencias de datos respecto a terceros países en el derecho de la Unión, que recoge el mecanismo de las decisiones de adecuación en el que se basaba el acuerdo entre la UE y EE.*U*U., con el objetivo de determinar los requisitos que lo componen. Posteriormente, se presentarán los antecedentes con el acuerdo del *Safe Harbor* y el caso *Schrems I*, planteando el panorama previo al Escudo de Privacidad, marcado por las dudas e inseguridades sobre el acuerdo. Finalmente, se examinará la sentencia del caso *Schrems II* describiendo las circunstancias del

correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO L 215, de 26 de julio del 2000).

8 Edward Snowden, antiguo empleado de la Central Intelligence Agency y de la National Security Agency, publicó a través de los periódicos de *The Guardian* y *The Washington Post* documentos clasificados sobre las actividades de los diferentes servicios de información de EE.UU., en los que se constataba la existencia de programas masivos de vigilancia global. Disponible en: https://bit.ly/2OgOxiV.

9 Sentencia de 6 de octubre de 2015, Schrems I, C-362/14, EU:C: 2015:650 (en adelante *Schrems I*).

10 Decisión de ejecución (UE) 2016/1250 de la comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. (DO L 207, de 12 de julio de 2016).

11 Sentencia de 16 de julio de 2020, Schrems II, C-311/18, EU:C: 2020:559 (en adelante *Schrems II*).

proceso, y analizando la sentencia en clave crítica, para terminar con una serie de conclusiones.

II. UNA CONTEXTUALIZACIÓN SOBRE LA REGULACIÓN DE LAS TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES EN EL DERECHO EUROPEO

La protección de los datos de carácter personal y el respeto a la vida privada son derechos fundamentales clave en una sociedad digitalizada como la actual. Desde la UE se ha insistido en lograr un equilibrio entre la seguridad y la tutela de los derechos humanos. Concretamente el art. 16 del Tratado de Funcionamiento de la Unión Europea[12] (TFUE) establece que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan, y que el Parlamento Europeo y el Consejo establecerán las normas sobre la protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del derecho de la Unión, y sobre la libre circulación de estos datos. Asimismo, los arts. 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea[13] (CDFUE) reconocen el respeto a la vida privada y la protección de datos de carácter personal como derechos fundamentales íntimamente conectados pero independientes.

Estos objetivos han dado lugar a una serie de instrumentos legislativos en esta materia, de los cuales serán examinados de forma resumida en este epígrafe aquellos relevantes para la resolución del conflicto entre la UE y EE.UU., en lo referente a las transferencias internacionales de datos.

1. ESPECIAL MENCIÓN AL CONVENIO 108 COMO INSTRUMENTO INTERNACIONAL PRECURSOR Y SU RELEVANCIA EN LA PROTECCIÓN DE DATOS

Como se adelantaba previamente, en la actualidad el Convenio 108 del Consejo de Europa es el único instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos, cuya firma se abrió en primera instancia en 1981 de manera previa a la era de internet. En virtud de este convenio, las partes deben adoptar las medidas necesarias en su derecho

[12] DO C 326, del 26 de septiembre de 2012.
[13] DO C 364, de 18 de diciembre de 2000.

nacional, para que puedan aplicarse sus principios, con el objetivo de garantizar en su territorio el respecto de los derechos humanos fundamentales en el ámbito de la aplicación de la protección de datos. El convenio justifica su razón de ser en la necesidad de evitar un control excesivo que interfiera con el libre flujo internacional de información[14]. Y dedicó inicialmente su art. 12 al flujo transfronterizo de datos; concretamente, en su párrafo segundo se establecía la norma general de prohibición de que las partes del convenio pudieran restringir las transferencias internacionales de datos.

No obstante, el párrafo tercero preveía la facultad de establecer una excepción a esta norma mediante dos supuestos. El primero, en la medida en que su legislación previese una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra parte estableciese una protección equivalente, es decir, tenía que haber en ambos Estados garantías equivalentes con relación a protección de datos. Mientras que, la segunda excepción, implicaba que se podría restringir el flujo de datos cuando la transmisión se llevase a cabo desde su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la parte.

En 2001, el Consejo de Europa adoptó un protocolo adicional cuyo art. 2, bajo la rúbrica de «Transferencia de datos personales a destinatarios no sometidos a la competencia de las Partes del Convenio», preveía esta posibilidad, únicamente si dicho Estado u organización aseguraba un adecuado nivel de protección. Si bien, el párrafo segundo permitió autorizar la transferencia de datos personales sin la necesidad de un nivel adecuado de protección cuando el derecho interno así lo estableciese a causa de intereses concretos del afectado, o intereses legítimos (especialmente de carácter público); o bien, si se preveían las suficientes garantías, que pudiesen resultar de cláusulas contractuales por parte del responsable del tratamiento responsable de la transferencia y dichas garantías se considerasen adecuadas por las autoridades competentes de conformidad con el derecho interno.

Así hasta llegar al 2018, año en el que se adoptó un protocolo modificativo que lo actualizó, dando lugar al Convenio 108+, con el objetivo de proporcionar respuestas a los nuevos retos tecnológicos. Respecto a las transferencias internacionales de datos contempla que cuando un país destinatario no

[14] Así lo contempla el párrafo noveno del «Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data» del Consejo de Europa, 28-1-1981. Disponible en: https://rm.coe.int/16800ca434

se encuentre sujeto a la jurisdicción de una parte se requiere que se garantice un nivel adecuado de protección de datos. Se establecen dos medios principales para garantizar que el nivel de protección sea el adecuado, o bien por ley, o a través de salvaguardas estandarizadas o aprobadas que resulten legalmente vinculantes y ejecutables. Es decir, las cláusulas contractuales tipo o las reglas corporativas vinculantes. Actualmente hay 55 Estados parte en este convenio, incluida la UE, pero no EE.UU., que tiene la condición de observador.

2. LAS DECISIONES DE ADECUACIÓN DESDE LA DIRECTIVA 95/46 HASTA EL RGPD. EL PROBLEMA EN TORNO AL NIVEL ADECUADO DE PROTECCIÓN DE DATOS

Entrando ya en los propios actos legislativos de la UE en esta materia, y que han venido estableciendo un marco más claro sobre la protección de datos y los mecanismos para las transferencias internacionales, resulta primordial dedicarle las primeras líneas a la derogada Directiva 95/46, cuyo objetivo principal fue la armonización legislativa, así como ampliar y concretar el ámbito de protección de datos que había sido marcado por el Convenio 108. Con ella, se buscó que todos los Estados miembros implementasen un estándar de protección de datos a nivel europeo, constituyendo un ejemplo de progreso en la uniformización jurídica (De Miguel Asensio, 2004: 400). Concretamente, su art. 25 determinó una serie de principios en la cesión de datos a terceros países, establecidos fuera de la UE, que implicaban fundamentalmente que esta debía ser acorde al derecho nacional y que el país que recibiese esos datos debía tener un nivel de garantía adecuado, introduciendo este término por primera vez en el ámbito de la UE.

Ahora bien, en caso contrario la transferencia de datos en principio no podría llevarse a cabo, sistema que generó de cierta forma un «cortafuegos» para los datos personales de los ciudadanos de la UE, mientras que su apartado segundo estableció la decisión de adecuación o modelo de adecuación como mecanismo principal para la realización de transferencias. Esta decisión consiste en realizar una evaluación específica del país al que se va a realizar la transferencia internacional de datos. Junto al anterior, el art. 26, a su vez, proporcionaba una serie de casos excepcionales en los que se podría llevar a cabo la transferencia. Si bien, debe tenerse en cuenta que estos modelos de adecuación no son los únicos, pues existen otros mecanismos alternativos relativos a las garantías adoptadas por los responsables del tratamiento, como las cláusulas contractuales modelo, las normas corporativas vinculantes o excepciones específicas como el consentimiento del interesado, entre otros. Comparado con estos otros instrumentos, el sistema de la decisión de adecuación presenta una ventaja clara, y es que se trata de un acto jurídico

vinculante que tiene eficacia directa en los Estados miembros, que permite la transferencia integral a los países que han recibido el nivel de adecuación, pero como inconveniente principal cabe resaltar que se requiere un proceso largo hasta el reconocimiento (Recio Gayo, 2019). En consecuencia, las decisiones de adecuación de la Comisión Europea suponen el estándar más alto al requerir que el sistema legal del tercer país sea sustancialmente equivalente (Kuner, 2017) y el medio más eficaz debido al «aval» que está aportando la valoración de la Comisión Europea.

Sin embargo, como puede apreciarse, el término de nivel adecuado incluido en la Directiva 95/46 no llegó a definirse, solamente el considerando 56 aludía a que el nivel adecuado debía apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias. Se señaló que la «adecuación» constituía un importante punto de partida para las decisiones de la Comisión sobre adecuación; sin embargo, estos criterios no se formularon con precisión ni se aplicaron siempre de manera rígida (Bygrave, 2014: 30). Esta falta de definición generó una problemática en torno a si el término «adecuado», que debía corresponderse a un nivel de protección idéntico al otorgado por el ordenamiento jurídico de la UE en materia de protección de datos personales. Ante esta situación, en 1998, el Grupo de Trabajo del Artículo 29 (en adelante GT29)[15] elaboró una serie de criterios para una mejor aplicación del concepto de nivel adecuado[16]. En dicho documento se contemplaba la necesidad de considerar no solo el contenido de las normas aplicables a los datos personales transferidos a un tercer país, sino también el sistema empleado para asegurar la eficacia de las normas. Para ello, se tendría en cuenta un conjunto de principios básicos contemplados en el Convenio 108 y en la Directiva 95/46, como por ejemplo el principio de proporcionalidad y el de transparencia. Además, se requería distinguir los objetivos del sistema normativo de protección de datos, como el establecimiento de recursos ante posibles perjudicados o la asistencia en el ejercicio de derechos.

No obstante, no fue hasta 2015 cuando el TJUE en la sentencia del caso *Schrems I,* con la que se invalidó el *Safe Harbor*, determinó lo que

[15] 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).

[16] Véase Grupo de Trabajo del artículo 29,"Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", documento de trabajo adoptado por el Grupo de trabajo el 24 de julio de 1998; disponible en: https://bit.ly/2XZNIwx

implicaba el nivel adecuado de protección. Así, para establecer dicho nivel se debía comprobar cuán parecida era la regulación de ese tercer país con la europea. Se determinó que la expresión de nivel de protección adecuado debía entenderse en el sentido de una exigencia de 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 UE por la Directiva 95/46[17]. Es decir, que se requiere a los terceros países un nivel sustancialmente equivalente, pero no igual al que proporciona la legislación, si no uno menos fuerte, un nivel más próximo a la realidad. Su finalidad no es otra que permitir asegurar la continuidad del elevado estándar de protección de datos previsto en la UE.[18]

Posteriormente, en 2018, el RGPD tampoco incluyó una definición normativa sobre el nivel de adecuación. Sin embargo, y a diferencia de la Directiva 95/46, este reglamento sí que indica expresamente cuáles son aquellos factores que deben tenerse en cuenta para evaluar si un tercer país tiene un nivel adecuado o no. Su art. 45 establece que podrán realizarse transferencias de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, los sectores o la organización internacional traten de garantizar un nivel de protección adecuado mediante una decisión de adecuación. Incluyendo alternativas para aquellos casos en los que no exista dicha decisión, las garantías adecuadas, estas pueden ser aportadas por diferentes mecanismos, si bien el RGPD ha ampliado el abanico de instrumentos en los que se puede incluir y aportar dichas garantías adecuadas, incorporándose los códigos de conducta y los mecanismos de certificación, así como el reconocimiento de las normas corporativas vinculantes para los grupos multinacionales, aunque en la práctica se encontraban operativas (Ortega Giménez, 2019: 416), además de los citados previamente. La diferencia clave entre el régimen del RGPD y el de la Directiva 95/46 es que la única autoridad que va a poder declarar la idoneidad del país de destino de la transferencia por tener un nivel adecuado es la Comisión, sin que pueda recaer en los Estados miembros.

La evaluación de la Comisión Europea se elaborará sobre los elementos que enumera el art. 45.2, lo que le permitirá valorar adecuadamente la legislación, no declarar que la legislación del tercer Estado es igual que la contenida en el RGPD. Además, los medios a los que puede recurrir dicho Estado pueden

[17] Sentencia de 6 de octubre de 2015, Schrems I, C-362/14, EU:C: 2015:650, apdos. 74-76.

[18] Conclusiones del abogado general Yves Bot, Schrems/Data Protection Commisioner, C-362/14, EU:C: 2015:650, punto 72.

diferir de los implantados en la UE. No obstante, la adopción de una decisión de adecuación conllevará *a posteriori* un deber de supervisión por parte de la Comisión Europea de manera continuada sobre los acontecimientos de esos terceros países, sectores u organizaciones internacionales.

Por su parte, el considerando 104 contempla el marco general en el que se debe fundamentar dicha evaluación, concretamente en «los valores fundamentales en los que se basa la Unión, en particular la protección de los derechos humanos». En dicho marco, la Comisión tendrá en cuenta necesariamente numerosas circunstancias que, en resumen, tienen que garantizar un modelo de tutela efectiva de la protección de datos. Según la categorización de Piñar Mañas (2016: 442), los elementos de evaluación se dividen en tres grupos:

- El marco jurídico general en un sentido amplio. Aquí se encontraría la existencia de un Estado de derecho, la legislación, la jurisprudencia, los derechos efectivos y exigibles y el acceso a la justicia por los interesados cuyos datos personales sean objeto de transferencia a un tercer país. En cuanto al acceso a recursos administrativos o judiciales, se encuentra vinculado con el art. 47 de la CDFUE, que reconoce el derecho a la tutela judicial efectiva y al juez imparcial. Es importante destacar la referencia expresa al acceso de las autoridades a los datos personales y el garantizar las transferencias ulteriores de esos datos, en el art. 45.2 a). Esta última cuestión se encuentra íntimamente ligada al conjunto de circunstancias exigidas por el TJUE en la sentencia del caso *Schrems I*.
- La existencia y funcionamiento efectivo de una o varias autoridades de control, que tienen que cooperar con las autoridades de la UE y de los Estados miembros. En este punto el considerando 104 establece la exigencia de un control verdaderamente independiente, cuestión de gran relevancia debido a su directa conexión con el art. 8 de la CDFUE, que exige en su apartado tercero la existencia de una autoridad de control que garantice el respeto a las normas en esta materia.
- Finalmente, los compromisos internacionales asumidos sobre protección de datos, entre los que tiene gran importancia la adhesión al Convenio 108, como establece el considerando 105.

Estos elementos de evaluación contenidos en el marco del considerando 104 y en el art. 45.2 mantienen cierto componente genérico, por lo que el

Comité Europeo de Protección de Datos (CEPD)[19] ha mantenido las directrices actualizadas del GT29 dadas por el anterior documento de 1998[20], con el objetivo de ofrecer una orientación detallada en la obtención de la adecuación en torno a la evaluación del nivel de protección de los datos en terceros países. En particular, expone los principios básicos sobre protección de datos que deben estar presentes en el marco jurídico de un tercer país con la finalidad de garantizar una equivalencia esencial con el marco de la UE. Entre los principios se encontrarían la existencia de conceptos básicos sobre protección de datos, no tienen que ser iguales a los del RGPD, pero sí presentar ciertas similitudes, la existencia de bases legales que permitan el procesamiento de los datos de forma legal, justa y legítima, entre otros.

Desde la entrada en vigor de la Directiva 95/46 y hasta la actualidad con el RGPD, los terceros países que han obtenido una decisión de nivel adecuado son Andorra (19/10/2010), Argentina (3/6/2003), Canadá (20/12/2001), EE.UU. (la última el 12/7/2016 invalidada), Guernsey (21/11/2003), Isla de Man (28/4/2004), Islas Feroe (5/3/2010), Israel (31/1/2011), Jersey (8/5/2008), Nueva Zelanda (19/12/2012), Suiza (26/7/2000), Uruguay (21/8/2012) y Japón (23/1/2019).

En el caso de Canadá[21] y EE.UU.[22], las decisiones de adecuación han sido «parciales», evidenciando la flexibilidad de configuración que pueden

---

19 El Comité Europeo de Protección de Datos es un organismo de la UE a cargo de la aplicación del RGPD a partir del 25 de mayo de 2018. Este organismo proporciona una guía general para aclarar el RGPD, adopta conclusiones coherentes y asesora a la Comisión Europea.

20 Véase Grupo de Trabajo del artículo 29, «Referencias sobre adecuación», documento de trabajo adoptado por el Grupo de trabajo el 28 de noviembre de 2017, disponible en: https://bit.ly/2XZTfmN

21 Decisión de la Comisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *Personal Information and Electronic Documents Act* (DO L 2, de 20 de diciembre de 2001).

22 La primera, Decisión de la Comisión 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 de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO L 215, de 26 de julio de 2000) y la segunda, Decisión de ejecución (UE) 2016/1250 de Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU. (DO L 207, de 12 de julio de 2016).

adoptar las decisiones de adecuación. Canadá garantiza una protección adecuada para las transferencias a los destinatarios a través de su ley[23]. Sin embargo, las diferencias filosóficas y culturales subyacentes en las regulaciones de privacidad entre EE.UU. y la UE siempre han generado dudas sobre si realmente el primero cumplía con el nivel de adecuación (Carr, 2017: 20), pues el sistema normativo europeo refleja el concepto de intimidad como un derecho humano fundamental protegido por los diferentes gobiernos. Mientras, EE.UU. no cuenta con un marco único de protección y privacidad de datos, llegando a describirse como un *collage* de diferentes estatutos federales y estatales debido a la ausencia de reglas concretas y únicas que rijan las transferencias internacionales de datos (Grant, 2005). El planteamiento que presentan es eminentemente sectorial, en el que se mezcla legislación, reglamentación y autorregulación, es un sistema descentralizado. No obstante, se han ido promulgando normas a nivel federal que afectan a la protección de datos personales como, por ejemplo, *Children's Online Privacy Protection act* (COPPA por sus siglas)[24], que regulaba el método a través del cual las empresas o entidades pueden recabar datos de menores de trece años. O en 2001: tras los atentados terroristas del 11 de septiembre se promulgó la *USA Patriot Act*[25], que se trataba de una ley federal que tenía como objetivo principal la ampliación de capacidad de control del Estado otorgando a las distintas agencias de seguridad estadounidenses mayor poder de vigilancia en la lucha contra el terrorismo.

Esto, unido a las revelaciones efectuadas en 2013 de que la National Security Agency norteamericana había estado llevando a cabo una vigilancia electrónica masiva generalizada, provocaron un extenso debate mundial sobre la privacidad (Cole y Fabbrini, 2016), y que la UE condenase que la protección de los datos de carácter personal que ofrecía EE.UU. era manifiestamente insuficiente (Maqueo Ramírez *et al.*, 2017: 78-85), situación que culminó en su día con la invalidación del *Safe Harbor.*

Estas inseguridades se han agravado durante los últimos años tras la aparición de leyes como la *Cloud Act*[26], que permite el acceso de las autoridades norteamericanas a datos almacenados en servidores de empresas norteamericanas situados en el extranjero, al amparo de una orden judicial, todo ello por

---

23 *Personal Information Protection and Electronic Documents Act 2000, SC 2000, c.5, assented to 2000-04-13.*

24 *Children's Online Privacy Protection Act of* 1998, 15 U.S.C. 6501–6505.

25 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of* 2001, HR 3162 RDS.

26 *Clarifying Lawful Overseas Use of Data Act* o *Cloud Act*, 2018, HR 4943.

razones de seguridad nacional y sin tener que cumplir con ninguna normativa de privacidad ni tampoco de protección de datos europea[27], demostrando una clara incompatibilidad con la regulación europea y generando tensiones en la práctica internacional (Cordero Álvarez, 2019: 80-100). Este convulso panorama ha terminado también con la invalidación del *Privacy Shield* en 2020, como analizaremos en las siguientes secciones.

III. EL PRIMER ACUERDO EN LA TRANSFERENCIA INTERNACIONAL DE DATOS. EL *SAFE HARBOR* Y EL CASO *SCHREMS I*

Las amplias relaciones comerciales a lo largo de los años entre la UE y EE.UU. han generado un elevado número de transferencias internacionales de datos, lo que derivó en su momento en la negociación entre el Departamento de Comercio estadounidense y la Comisión Europea de un acuerdo para la protección de dichos datos. El *Safe Harbor* o Puerto Seguro fue el primero, en virtud del cual los datos personales podían transferirse legalmente entre un Estado miembro de la UE y EE.UU., con fines comerciales. Este acuerdo reconoció los estándares de transferencia de datos a través de un sistema de autocertificación de empresas estadounidenses. Si las entidades cumplían una serie de principios podían obtener una certificación para poder llevar a cabo transferencias de datos con la UE bajo el amparo del acuerdo, y pasando a formar parte de una lista publicada de todas aquellas empresas que lo estuviesen. No obstante, los principios del Puerto Seguro podrían limitarse, en la medida necesaria, en atención a los requisitos de seguridad nacional, interés público o aplicación de la ley.

Se promovió en el ámbito norteamericano la autorregulación al dejar que las empresas decidiesen si adoptar o no los principios europeos, pues la UE reconoció la realidad política de EE.UU. y la improbabilidad de la promulgación de un estatuto general de privacidad. Precisamente, el hecho de que tuviera un carácter autocertificativo y el espíritu poco europeo de sus preceptos suscitó diversas críticas a lo largo de los años (Darcy, 2015: 131). Además, tras las divulgaciones en junio de 2013 de los programas de vigilancia

[27] Esta modificación legislativa tiene su origen en el caso entre Microsoft y el Gobierno de los EE.UU. iniciado en 2013 (*United States v. Microsoft Corp.,* 138 S. Ct. 356, 2017), en atención a la pretensión del Gobierno estadounidense de acceder a los datos de una persona objeto de investigación, alojados en un servidor de la compañía situado en Irlanda. Antes de que pudiera ser resuelto por el Tribunal Supremo de EE.UU., la *Cloud Act* fue adoptada, dejando sin causa al Tribunal.

de la *National Security Agency* de EE.UU. y denuncias posteriores de otras actividades de inteligencia de EE.UU. en Europa, la Comisión advirtió que muchas empresas autocertificadas no cumplían con los principios del *Safe Harbor*. Esto se hizo a través de varias comunicaciones al Parlamento Europeo y al Consejo en las que se señaló que este incumplimiento permitió a las autoridades estadounidenses acceder a los datos personales transferidos y tratarlos de manera incompatible con las finalidades establecidas[28]. Ante la magnitud de la problemática, afloraron las dudas en la UE sobre la capacidad de protección de los datos personales de los ciudadanos europeos, ya que tanto la normativa del país como sus prácticas no garantizaban una protección adecuada sobre los datos que se le transferían frente a las actividades de vigilancia por las autoridades (Ortega Giménez, 2017: 86).

Esta situación terminó desembocando en la sentencia *Schrems I* de 2015, que marcó un hito en la historia de las decisiones de adecuación. En este caso, Maximillian Schrems, un estudiante de derecho austriaco y usuario de Facebook, presentó una denuncia ante el Comisionado de Protección de Datos de Irlanda, tras las revelaciones del antiguo agente de la Central Intelligence Agency Edward Snowden, de que la Agencia de Seguridad Nacional de Estados Unidos había accedido a servidores de varias empresas estadounidenses, argumentando que el Puerto Seguro no proporcionaba una protección adecuada desde la vigilancia por parte de las autoridades públicas de personas y empresas.

El TJUE confirmó que EE.UU. participaba en una vigilancia masiva indiscriminada de los ciudadanos europeos y que el *Safe Harbor* no proporcionaba un nivel adecuado de protección. La interpretación realizada por el TJUE le llevó a concluir que el *Safe Harbor* permitía la injerencia en los derechos fundamentales de los ciudadanos europeos por parte de las autoridades norteamericanas y la existencia de una falta de control jurisdiccional por parte de EE.UU. frente a la protección de datos. Se aclaró el alcance de las facultades de las autoridades de protección de datos, incidiendo en que están investidas de la competencia para comprobar si una transferencia de datos personales desde el Estado miembro de esa autoridad respeta las exigencias establecidas, en este caso, por la anterior Directiva 95/46. Las autoridades de control ante las que se presentase una solicitud debían poder apreciar con toda independencia si esa transferencia de datos cumple las exigencias

[28] Véase Comunicación de la Comisión al Parlamento Europeo y al Consejo, «Restablecer la confianza en los flujos de datos entre la UE y EE.UU.», COM (2013) 0846 final, 27 de noviembre de 2013.

establecidas, suspendiéndola en caso contrario y dirigiéndose a los tribunales para que planteen una cuestión prejudicial (Álvarez y Recio, 2016: 133).

La decisión del *Safe Harbor* presumía que EE.UU. cumplía con el estándar de nivel de protección adecuado exigido por la anterior directiva, y en este sentido, el TJUE valoró dicho estándar conforme a los criterios del art. 25.2. Para satisfacerlo, el Tribunal estimó que el tercer país podía ofrecer medios distintos de protección, pero en la práctica su nivel de eficacia debía ser sustancialmente equivalente al nivel de protección asegurado en la UE[29]. Con el fin de determinar si se había producido una infracción en el derecho a la privacidad se realizó una valoración del ordenamiento jurídico interno de EE.UU. Aunque *a priori* el sistema de autocertificación no era contrario al estándar, el Tribunal consagró la existencia de la primacía de las exigencias de seguridad nacional y de la legislación interna estadounidense sobre los principios de puerto seguro. Esto provocaba una evidente injerencia por parte de las autoridades estadounidenses en la vida privada de los ciudadanos europeos, ya que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el derecho a la vida privada.

La sentencia *Schrems I* también consideró que se había vulnerado el contenido esencial del derecho a la tutela judicial efectiva. La existencia de un control jurisdiccional efectivo para garantizar el cumplimiento del derecho de la UE es inherente al Estado de derecho. Y el derecho norteamericano no contemplaba recursos judiciales eficaces para que los ciudadanos europeos pudiesen alegar una vulneración de sus derechos fundamentales en relación con sus datos personales. Por ello, el contenido esencial del derecho a la tutela judicial efectiva resultó claramente vulnerado.

El TJUE determinó que en este caso no se cumplía con los requisitos del nivel adecuado de protección y, por lo tanto, el *Safe Harbor* no proveía una base legal para las transferencias de datos entre la UE y EE.UU. La sentencia de *Schrems I* demostró que este mecanismo de decisiones tenía debilidades, llegando al punto de ser insuficientes para la protección de la privacidad de los ciudadanos europeos, y que en ocasiones podría no haber un nivel adecuado de protección.

Tras este caso, se abrió un futuro incierto, vinculado a las grandes diferencias entre los modelos de protección de datos prevalentes en EE.UU. y la UE (Ni Loidean, 2016: 3), cuya coordinación se vio dificultada por las revelaciones relativas a las actividades de supervisión llevadas a cabo

[29] Conclusiones del abogado general Yves Bot, Schrems/Data Protection Commisioner, C-362/14, EU:C: 2015:650, punto 120.

por las autoridades de EE.UU. y que provocó que la UE condenase la falta de protección (Roth, 2017: 49). Se generó una tensa inseguridad jurídica e incertidumbre, pues tras una vigencia de quince años se requerían unas pautas claras para que responsables y encargados del tratamiento supiesen cómo efectuar las transferencias. Quedó claro en los meses posteriores a la sentencia que la única solución a la invalidez del sistema del *Safe Harbor* como marco habilitante de las transferencias entre la UE y los EE.UU. pasaba por encontrar un acuerdo.

El refuerzo a la eficacia extraterritorial del derecho fundamental a la protección de los datos personales de los ciudadanos europeos que se alcanzó a través de la sentencia no podría, sin embargo, dejar en situación de desamparo a las empresas europeas, que no gozaban de alternativas fáciles (De Miguel Asensio, 2015: 1-10). Esto propició nuevas negociaciones para la creación de un nuevo acuerdo, el *Privacy Shield*.

La influencia provocada tras este caso y el papel que la UE ha ido desempeñando en el sector de la protección de datos, sumado al alcance del RGPD, ha acabado provocando ciertos cambios en varios Estados de EE.UU., ya que se están introduciendo leyes de privacidad con diversas similitudes. De entre ellos, en el Estado de California la *California Consumer Privacy Act*[30] (CCPA por sus siglas) es la de mayor alcance, cuya entrada en vigor se produjo el 1 de enero de 2020. La CCPA se basa en varios principios de privacidad establecidos con el RGPD, otorgando a sus ciudadanos la posibilidad de conocer qué datos han recopilado las diversas compañías sobre ellos, impedir a las compañías que vendan sus datos y solicitar que se eliminen. Además, están trabajando en otra iniciativa legislativa para crear un Agencia de Protección de la Privacidad en California.

Sin embargo, como se analizará posteriormente, y a pesar de los precedentes marcados por la *Schrems I* sobre las limitaciones del *Safe Harbour* y los avances en la legislación de diferentes Estados norteamericanos, el *Privacy Shield* terminaría por invalidarse con la sentencia *Schrems II*.

IV. LA DECISIÓN DEL ESCUDO DE PRIVACIDAD Y SU ANULACIÓN CON LA SENTENCIA *SCHREMS II*

La invalidación del sistema del *Safe Harbour* puso de manifiesto la necesidad de encontrar y alcanzar un nuevo acuerdo político entre la UE y EE.UU., que culminó el 2 de febrero de 2016 con el establecimiento de un nuevo marco para las transmisiones de datos personales entre ambos.

30 *California Consumer Privacy Act of* 2018 [1798.100 - 1798.199.100].

Seguidamente, el 29 de febrero la Comisión Europea hizo público un proyecto de decisión sobre la idoneidad del nuevo marco y sus anexos, que incluían una serie de compromisos y declaraciones por parte de las autoridades norteamericanas. Dichos compromisos fueron evaluados por instituciones especializadas en la materia, y condujeron finalmente a la adopción el 12 de julio de 2016 del acuerdo denominado *Privacy Shield* o Escudo de Privacidad tras más de dos años de negociación.

El objetivo principal del acuerdo fue proveer una equivalencia esencial al RGPD. Para ello, se vuelve a adoptar el sistema de autocertificación y se incluyen, en gran medida, los mismos principios que se encontraban en el *Safe Harbor*. El Departamento de Comercio estadounidense es responsable de gestionar y administrar el *Privacy Shield* y de garantizar que las empresas respeten sus compromisos. Para disponer de certificación, las empresas deben contar con una política de privacidad acorde con los principios de privacidad, así como renovar anualmente su afiliación al Escudo de Privacidad. En caso de no hacerlo, ya no podrán recibir y usar datos personales de la UE conforme a este marco.

Aunque *a priori* se mantenga el mismo esquema que el empleado por el Puerto Seguro, se hicieron varias reformas sustanciales en el nuevo acuerdo. Una de las más destacadas fue que los operadores bajo el Escudo de Privacidad se encontraban sujetos a compromisos con respecto a los límites de retención de datos, derechos de acceso, publicidad de políticas de privacidad, etc. Respecto al funcionamiento de los poderes públicos estadounidenses, la adhesión a los principios se limita a lo estrictamente necesario para satisfacer las exigencias de seguridad nacional, interés público o aplicación de la ley. Además, el Gobierno estadounidense se comprometió a crear un mecanismo de supervisión de las injerencias con fines de seguridad nacional, el Defensor del Pueblo. Esta figura se implementó dentro del Departamento del Estado, y era el responsable de la investigación de los casos presentados por las autoridades europeas en protección de datos. Otra de las novedades que introdujo el Escudo de Privacidad fue en su ámbito de aplicación, pues afecta tanto a las transferencias internacionales de carácter comercial como al acceso de las autoridades públicas de EE.UU. a los datos transferidos desde la UE, incluso por causas de seguridad nacional. Aunque esto no evitó que a nivel práctico siguiese prevaleciendo la normativa estadounidense en dicho ámbito y su eficacia estuviese llena de matices.

A pesar de las mejoras, el acuerdo no cumplió desde el inicio con los estándares requeridos (Blasi Casagran, 2017: 198-205), recibiendo críticas y

negativas por parte del anterior GT29[31] ya que detectó ciertas debilidades en el *Privacy Shield*. Fundamentalmente, que el texto no obligaba a las entidades adheridas al borrado de los datos cuando ya no resultan necesarios, lo que suponía la infracción de que los datos no debían almacenarse por más tiempo del estrictamente necesario para cumplir la finalidad por la que fueron recopilados.

Un segundo problema fue que el gobierno de EE.UU. se amparaba en las excepciones por motivos de seguridad y no excluía de forma total la posibilidad de que se recopilasen de forma masiva datos personales de ciudadanos europeos. Finalmente, la última cuestión controvertida era la relativa al mecanismo de reparación extrajudicial para los interesados, ya que no se indicaba cómo se garantizaba la independencia del organismo que se encargase o el poder suficiente para que pudiera ejercer sus funciones de forma efectiva.

La renovación del acuerdo y las revisiones anuales positivas llevadas a cabo por la Comisión resultaron insuficientes y persistieron las dudas sobre que el *Privacy Shield* no tuvo nunca en cuenta la evaluación realizada por la Comisión sobre las normas de protección de datos de EE.UU. (Terpan, 2018:1045). Aun así, faltaba una valoración adecuada, una de las principales motivaciones en *Schrems I*, y como no se había corregido, había evidencias para creer que la vigencia del Escudo de Privacidad seguía siendo frágil (Tracol, 2016: 775). Desde este punto de vista, el *Privacy Shield* siempre fue una actualización moderada que heredó en parte los problemas que tenía su antecesora.

1. LOS HECHOS QUE DIERON LUGAR A LA SENTENCIA

El caso de Maximillian Schrems no terminó tras la sentencia del 2015, pues las actuaciones procesales se retrotrajeron al momento de su reclamación ante el Comisionado de Protección de Datos de Irlanda, cuya investigación puso de manifiesto que una gran parte de los datos personales que se encontraban alojados en Facebook Ireland se transfería a la sede en EE.UU. mediante cláusulas contractuales tipo (en adelante CCT) de protección de datos recogidas en el anexo de la Decisión de la Comisión 2010/87/UE (en adelante Decisión CPT)[32], pero contenidas en uno de los anexos de la decisión de ejecución del Escudo de Privacidad.

---

31 Véase Grupo de Trabajo del Artículo 29, «Opinion 01/2016 on the EU- U.S Privacy Shield draft adequacy decisión», adoptada el 13 de abril de 2016, disponible en: https://bit.ly/38yG3uu.

32 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 trata-

Ante esta situación, el señor Schrems modificó su reclamación alegando que el derecho norteamericano obligaba a Facebook Inc. a poner los datos personales que se le transfiriesen a disposición de las autoridades como la Agencia de Seguridad Nacional o la *Federal Bureau of Investigation* (FBI), y que podrían ser usados en el marco de diferentes programas de vigilancia de forma incompatible con los arts. 7, 8 y 47 de la CDFUE. Tras esta investigación, el Comisario publicó la investigación en mayo de 2016 con la que estimó que las CCT recogidas en la Decisión CPT no subsanaban las deficiencias de protección de aquellos datos transferidos a EE.UU.

Ante esta situación se inició un procedimiento ante la High Court en Irlanda, que planteó la petición de decisión prejudicial, incluyendo además una sentencia nacional que analizaba las actividades de inteligencia de las autoridades estadounidenses en lo referente a los datos personales transferidos desde la UE, lo que llevó a plantear una serie de cuestiones prejudiciales. De entre ellas, el TJUE determinó resolver la interpretación del art. 3, apdo. 2, primer guion, de la Directiva 95/46 en relación con el art. 4 TFUE, apdo. 2, y los arts. 7, 8 y 47 de la CDFUE; la interpretación y la validez de la Decisión CPT; y finalmente, la interpretación y validez del *Privacy Shield.*

2. LOS FUNDAMENTOS DE LA DECLARACIÓN DE INVALIDEZ DEL ESCUDO DE PRIVACIDAD Y LA CONTINUIDAD DE LAS CLÁUSULAS TIPO DE PROTECCIÓN DE DATOS

El TJUE ha apreciado, como ocurrió en 2015, que la constatación realizada por la Comisión en el *Privacy Shield* de que EE.UU. garantiza de forma efectiva un nivel sustancialmente equivalente con el ordenamiento jurídico de la UE para las transferencias de datos no se corresponde con la realidad. Fundamentalmente, y en una relación claramente directa con los requisitos para el nivel adecuado de protección previamente analizados, los derechos fundamentales afectados son los contemplados en los arts. 7, 8 y 47 de la CDFUE. Y es que el TJUE ha podido examinar las limitaciones de los principios debido a las exigencias de seguridad nacional, interés público y cumplimiento de la normativa. Constatando que la decisión admite con carácter general este tipo de injerencias por parte de las autoridades estadounidenses, concretando que dichas intrusiones pueden producirse como consecuencia del acceso a los datos personales transferidos desde la UE a EE.UU. y de

miento establecidos en terceros países, de conformidad con la Directiva 95/46, en su versión modificada por la Decisión de Ejecución (UE) 2016/2297 de la Comisión, de 16 de diciembre de 2016 (DO 39, de 5 de febrero de 2010).

la utilización de esos datos por las autoridades públicas estadounidenses, en el marco de los programas de vigilancia norteamericanos[33], conforme a los arts. 702 de la *Foreign Intelligence Surveillance Act* (en adelante FISA) y en la *Executive Order* 12333 (en adelante E.O. 12333)[34]. A este respecto, el TJUE considera que la normativa de EE.UU. no prevé las limitaciones y garantías necesarias en atención a dichas injerencias, ni tampoco garantiza la tutela judicial efectiva frente a ellas[35]. A esto último debe sumarse que el Tribunal considera que la figura creada por el Escudo de Privacidad, el Defensor del Pueblo, no puede subsanar su carencia ya que no es un verdadero tribunal[36].

Resulta jurisprudencia asentada que la comunicación de datos de carácter personal a un tercero, como puede ser una autoridad pública, constituye una injerencia en los derechos fundamentales de los arts. 7 y 8 de la CDFUE, con independencia del uso posterior de la información[37]. Sin embargo, esta interpretación del TJUE no olvida que estos derechos no son absolutos y que pueden verse limitados, entrando en juego el principio de proporcionalidad. Es decir, que las limitaciones podrán introducirse cuando sean necesarias y respondan efectivamente a los objetivos de interés general reconocidos por la UE o a la necesidad de protección de los derechos y libertades de los demás, debiendo estar establecida por ley. El requisito de proporcionalidad requiere que la normativa que conlleve la injerencia establezca reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, incluyendo de esta forma garantías suficientes para

---

33 Los dos programas más famosos son PRISM y Upstream. PRISM es una herramienta utilizada por la National Security Agency, para recoger datos electrónicos privados pertenecientes a los usuarios de los principales servicios de Internet como Gmail, Outlook o Facebook. Mientras que Upstream implica la interceptación del tráfico telefónico y de Internet de los principales cables y conmutadores, tanto nacionales como extranjeros.

34 *Foreign Intelligence Surveillance Act* de 1978 (FISA) (Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. cap. 36), la ley federal que establece los procedimientos de vigilancia física y electrónica y recopilación de información de inteligencia extranjera. *Executive Order* 12333 *of Dec*. 4, 1981, *appear at* 46 FR 59941, 3 CFR, destinada a ampliar poderes y responsabilidades de las agencias de inteligencia estadounidenses.

35 Sentencia de 16 de julio de 2020, *Schrems II*, C-311/18, EU:C: 2020:559, apartados 180-185.

36 Sentencia de 16 de julio de 2020, *Schrems II*, C-311/18, EU:C: 2020:559, apartados 194-198.

37 Véanse las sentencias de 20 de mayo de 2003, *Österreichischer* Rundfunk y otros, C-465/00, C-138/01 y C-39/01, EU.C:2003:294; y de 8 de abril de 2014, *Digital Rights Ireland y otros*, C-293/12 y C-594/12, EU:C:2014:238.

los interesados. Por lo tanto, el TJUE, tras el examen de los programas de vigilancia citados anteriormente, determina que no pueden garantizar un nivel de protección sustancialmente equivalente, por lo que las autoridades públicas pueden acceder y utilizar los datos sin encontrarse sujetos al principio de proporcionalidad. Tanto el asunto *Schrems I* como el *II* vienen a continuar con la tarea de someter las actividades de los servicios de inteligencia dirigidas a combatir el terrorismo mediante la aplicación de los criterios de proporcionalidad (Lucas Murillo de la Cueva, 2020: 6).

Respecto a esta última cuestión, estaba pendiente otro caso, *Privacy International*[38], con el que el TJUE ha determinado que la transmisión generalizada e indiferenciada de datos por parte de los proveedores de servicios de comunicaciones electrónicas para su comunicación a las agencias de seguridad e inteligencia excede los límites de lo necesario y resulta contrario a la CDFUE. Una decisión en la misma línea es el de *La Quadrature du Net*[39], cuya sentencia fue publicada en octubre de 2020, y en la que el TJUE incide en que para cumplir el requisito de proporcionalidad, las limitaciones al ejercicio de los derechos fundamentales deben contar con una base legal que defina su alcance, sin sobrepasar los límites de lo estrictamente necesario y estableciéndose los requisitos materiales y procedimentales que regulen la utilización. El TJUE reconoció que hay determinadas situaciones en las que un Estado miembro se puede enfrentar a una seria amenaza frente a la seguridad nacional, y cuando esta sea real y actual o previsible, cumpliéndose en este caso el requisito de proporcionalidad[40]. Estas sentencias refuerzan los límites y controles de la capacidad de vigilancia de las autoridades públicas, pudiendo eventualmente tener un efecto relevante en el futuro de las decisiones de adecuación frente a terceros Estados, ya que la evaluación que deberá hacer la Comisión conforme al RGPD se verá condicionada al tener que examinar los ulteriores tratamientos a los que puedan verse sometidos los datos transferidos por las autoridades de dicho Estado ante fines de seguridad pública (De Miguel Asensio, 2020: 3).

En cuanto a la cuestión de la tutela judicial efectiva recogida en el art. 47 de la CDFUE, el TJUE reconoce que la existencia de un control jurisdiccional efectivo para garantizar el cumplimiento de las disposiciones del derecho de la UE resulta inherente al Estado de derecho. Por ello, como ya anunciaba en el

---

38 Sentencia de 6 de octubre de 2020, *Privacy International,* C-623/17. EU:C:2020:790, apdos. 76-82.

39 Sentencia del Tribunal de Justicia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18. EU:C:2020:791, apdos. 175 y 176.

40 Sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apdo. 177.

caso *Schrems I*, una normativa que no prevé la posibilidad de que el interesado pueda ejercer acciones en derecho en lo referente a sus datos personales está incumpliendo con el derecho a la tutela judicial efectiva.

Esta interpretación se plantea al hilo de determinar si la existencia del mecanismo del Defensor del Pueblo, establecido por las autoridades estadounidenses, podría suplir los problemas relativos al planteamiento de acciones administrativas o judiciales para la defensa de los interesados. A lo que el TJUE contesta negativamente ya que, por una parte, al formar el Defensor del Pueblo parte del Departamento de Estado, se pone en entredicho la independencia de este con respecto al poder ejecutivo y, por otra parte, esta figura no está dotada de facultades para adoptar decisiones vinculantes respecto a los servicios de inteligencia (ante posibles infracciones) ni tampoco garantías que puedan ser invocadas por los interesados. Surge nuevamente el mismo planteamiento de 2015, se requiere que existan mecanismos que sean eficaces para la detección y control de posibles violaciones del derecho a la protección de datos en EE.UU.; sin embargo, no se traducen en la realidad.

El análisis del TJUE sobre las garantías adecuadas proporcionadas por las CCT ha sido el otro argumento trascendental del caso. En este sentido, Ruíz Tarrías (2020: 145) señala que pueden diferenciarse dos aspectos esenciales: por una parte, el reconocimiento de diferentes facultades a las autoridades de control independientes con el objetivo de valorar el nivel de protección adecuado ofrecido por el tercer país, en atención al instrumento de licitud en el que se basa la transferencia internacional de datos personales. El TJUE considera, por lo tanto, como en *Schrems I*, que aunque haya una decisión de adecuación la autoridad nacional de control puede tramitar reclamaciones de los particulares para proteger sus derechos frente al tratamiento de datos y en caso de que la transferencia no cumpla con las exigencias del RGPD, interponer un recurso ante los tribunales nacionales[41]. Mientras que cuando las transferencias tengan su fundamento en otro mecanismo, como las CCT, las autoridades nacionales de control tienen reconocida la facultad de prohibir o suspenderla cuando verifiquen que se están llevando a cabo infringiendo la normativa europea o la legislación nacional en protección de datos[42].

Y, por otra parte, la aserción de que no existen diferencias entre las decisiones de adecuación y las CCT respecto a la exigencia de cumplimiento de garantías adecuadas en atención a los elementos contemplados en el

[41] Sentencia de 16 de julio de 2020, Schrems II, C-311/18, EU:C: 2020:559, apdos. 119-120.

[42] *Ibid.*, apdos. 115-121.

art. 45.2 RGPD, aun cuando el TJUE formule sobre ello argumentos contradictorios que terminen por diferencias en este aspecto a estos dos mecanismos.

Estas consideraciones son las que llevan al TJUE a declarar inválida la decisión del Escudo de Privacidad, confirmando que el *Privacy Shield* no había tenido en cuenta las críticas y recomendaciones llevadas a cabo a lo largo del tiempo. Esta sentencia ha venido a finalizar un debate que llevaba abiertos años sobre una de las decisiones de adecuación más mediáticas, considerando que la primacía de las exigencias sobre la seguridad nacional, el interés público y el cumplimiento de la ley estadounidenses posibilitaban injerencias en los derechos fundamentales de los ciudadanos europeos. Y al mismo tiempo, no proporcionaba a los posibles afectados vías de recurso ante un órgano con garantías suficientes.

Por otro lado, ha desaparecido la posibilidad de que aquellos que transfiriesen datos personales desde la UE a una organización adherida al acuerdo en los EE.UU. puedan recurrir a este mecanismo como base legal, para proporcionar garantías suficientes. Es decir, que para poder seguir llevando a cabo transferencias de datos personales tendrán que aplicar las CCT u otra de las garantías recogidas en el RGPD.

Este planteamiento del TJUE afecta de lleno a la relación de la UE con el Reino Unido, en el marco del Brexit tras su salida definitiva en enero de 2021, ya que al convertirse en un Estado tercero requiere que se adopte alguno de los mecanismos del RGPD para la transferencia internacional de datos. Esto implica que, pasados los seis primeros meses de 2021, deberá existir una decisión de adecuación de la Comisión Europea o el establecimiento de alguno de los mecanismos de garantías adecuadas, como las CCT. No obstante, no podrá producirse dicha decisión si Reino Unido no proporciona un nivel adecuado de protección, como bien ha remarcado el TJUE. Cuestión que podría llegar a suceder, ya que en octubre de 2019 Reino Unido firmó con EE.UU. el primer acuerdo ejecutivo de la *Cloud Act: Data Access Agreement*, en virtud del cual en caso de delitos graves pueden exigir datos personales a compañías tecnológicas con sede en el otro país sin ningún tipo de barrera.

Las transferencias de datos personales entre la UE y EE.UU. llevan siendo un problema desde hace más de veinte años y seguirán siendo un problema mientras EE.UU. no adopte una normativa de privacidad que conlleve un estatus de adecuación o, como han apuntado otros autores, se establezca un marco de carácter internacional con estándares sobre la privacidad y la protección de datos (Martínez Martínez, 2020: 2). Casos como los

de Facebook y *Cambridge Analytica*[43], en el que se produjo una violación a escala mundial de los datos personales de los usuarios, no han hecho más que aumentar la inseguridad jurídica y las tensiones entre ambas potencias. Sin embargo, la UE ha desempeñado durante los últimos años un papel trascendental en la configuración de cómo ve el mundo la privacidad de los datos. Esta mentalidad ha ido adentrándose en el ámbito tecnológico y jugando un papel esencial en ese cambio, sobre todo tras la entrada en vigor del RGPD. Este cambio cultural está comenzando a apreciarse en la mentalidad empresarial de EE.UU., como el ejemplo comentado anteriormente en el Estado de California. A pesar de que la privacidad resulte cultural en muchos aspectos, lo que complica reflejar un estándar de privacidad de una región a otra, los diversos problemas y revelaciones acontecidos a lo largo de los años parecen estar modificándolo (Sobrino García, 2020: 8). Por ello, no resulta imposible que con el paso del tiempo el sistema jurídico norteamericano a nivel federal tienda a una estructura más compatible con establecida por la UE., si bien las diferencias en las perspectivas europea y estadounidense respecto a los límites en la lucha antiterrorista complican el panorama de las transferencias internacionales de datos.

V. CONCLUSIONES

Las transferencias internacionales de datos resultan claves en el desarrollo de la economía mundial actual. Por ello, la UE ha establecido mecanismos para que puedan llevarse a cabo con terceros países. Sin embargo, los conflictos por las diferencias normativas con otros países han creado inseguridades entre la ciudadanía europea. El caso más relevante es el estadounidense, en el que uno de los focos principales de problemas es la propia normativa interna norteamericana. El sistema legal de EE.UU. lleva considerando este tiempo la privacidad de la información como un interés del consumidor, mientras que en la UE es un derecho fundamental.

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

Aunque no resultaría beneficioso desde un punto de vista económico el bloqueo de transferencias internacionales, tampoco puede permitirse

[43] *United States of America before the Federal Trade Commission in the matter of Cambridge Analytica, LLC, a corporation,* DOCKET NO. 9383, el 22 de julio de 2019.

una vulneración de la privacidad de los ciudadanos europeos. El sistema de autocertificación de empresas no funciona como barrera de protección, pues en el caso de países como EE.UU., que no cuentan con una verdadera legislación en protección de datos, los datos de los ciudadanos europeos quedan expuestos a los sistemas de excepciones. Sin embargo, aunque se opte por otros mecanismos como las CCT la existencia de una normativa estadounidense que no cumple con el principio de proporcionalidad ni aporta garantías suficientes puede acabar afectando también a la validez de las transferencias por estos medios. Lo que requerirá la evaluación de todas las circunstancias de las transmisiones e incluso la adopción de medidas suplementarias que aporten una mayor protección, cuestión que pone de relieve la importancia del principio de *accountability* o de responsabilidad proactiva que encarna el RGPD.

En este sentido, la sentencia del TJUE traerá importantes consecuencias en las futuras y presentes decisiones de adecuación, como es el caso del Reino Unido tras su salida de la UE con del Brexit, pues puede no llegar a cumplir con el nivel adecuado de protección tras el acuerdo firmado con EE.UU. sobre el acceso a datos personales en el marco de delitos graves, no conteniendo las garantías necesarias que este tipo de limitaciones requieren. Como ha aclarado el TJUE en su sentencia *Schrems II*, una decisión de adecuación no podrá otorgarle primacía a las exigencias de seguridad nacional que supongan una injerencia ilegítima de las autoridades públicas en los derechos fundamentales de los ciudadanos europeos.

Las transferencias de datos transfronterizas entre la UE y EE.UU. seguirán siendo un problema, ya que no parece que EE.UU. adopte reglas de privacidad que puedan conducir a un estado de adecuación. Sin embargo, los cambios culturales tras la entrada en vigor del RGPD y las múltiples experiencias negativas por parte de EE.UU. en lo concerniente a la protección de datos podrían dar lugar a cambios legislativos tendentes a la creación de una normativa estatal sobre protección de datos debido a la presión del mundo empresarial.

Bibliografía

Álvarez Caro, M. y Recio Gayo, M. (2016). La declaración de invalidez del acuerdo de Puerto Seguro entre la UE y los EE. UU. por el TJUE (C-362/14). *Revista Española de Derecho Europeo*, 57, 107-136.

Bender, D. (2016). Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective. *International Data Privacy Law*, 6 (2), 117-138. Disponible en: https://doi.org/10.1093/idpl/ipw005.

Bennett, C. J. y Raab, C. (2003). *The Governance of Privacy. Policy Instruments in Global Perspective*. Cambridge: The Massachusetts Institute of Technology Press.

Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *Computer Law and Security Review*, 24 (6), 508-520. Disponible en: https://doi.org/10.1016/j.clsr.2008.09.001.

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

Bygrave, L. A. (2014). *Data Privacy Law: An international Perspective*. Oxford: Oxford University Press. Disponible en: https://doi.org/10.1093/acprof:oso/9780199675555.001.0001.

Carr, G. (2017). Privacy Shield or privacy mask? An análisis of European Data Protection Law in response to the Case of Maximillian Schrems v. Data Protection Commissioner and the implementation of the general data protection regulation. *Student Comparative European Law Review*, 1, 20-40.

Cole, D. y Fabbrini, F. (2016). Bridging the transatlantic divide? The United States, the European Union and the protection of privacy across borders. *International Journal of Constitutional Law*, 14 (1), 220-237. Disponible en: https://doi.org/10.1093/icon/mow012.

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.

Darcy, S. (2015). Battling for the Rights to Privacy and Data Protection in the Irish Courts. *Utrecht Journal of International and European Law*, 31 (80), 131-136. Disponible en: https://doi.org/10.5334/ujiel.cv.

De Miguel Asensio, P. A. (2004). La protección de datos personales a la luz de la reciente jurisprudencia del TJCE. *Revista de la Facultad de Derecho de la Universidad de Granada*, 7, 397-417.

De Miguel Asensio, P. A. (2015). Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia. *La Ley Unión Europea*, 31, 1-10.

De Miguel Asensio, P. A. (2020). Implicaciones de la declaración de invalidez del Escudo de privacidad. *La Ley Unión Europea*, 84, 1-5.

Grant, J. (2005). International data protection regulation Data transfer and Safe Harbor. *Computer Law and Security Report*, 21, 267-261. Disponible en: https://doi.org/10.1016/j.clsr.2005.04.010.

Kuner, C. (2017). Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, 18 (4), 881-918. Disponible en: https://doi.org/10.1017/S2071832200022197.

Lucas Murillo de la Cueva, P. (2020). Entrevista: El perpetuum mobile del derecho a la protección de datos: no solo mantenerlo, sino reforzarlo. *La Ley Privacidad*, 6, 1-16.

Maqueo Ramírez, M. S., Moreno González, J. y Recio Gayo, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho*, 30, 77-96. Disponible en: https://doi.org/10.4067/S0718-09502017000100004.

Martínez Martínez, R. (2020). Schrems II. Una breve reflexión desde los derechos fundamentales. *La Ley Privacidad*, 5. Disponible en: https://bit.ly/3biGY3Z.

Moslemzadeh Tehrani, P., Bin HJ Sabaruddin, J. S. y Ramathan, D. A. P. (2018). Cross border data transfer: Complexity of adequate protection and its exceptions. *Computer Law and Security Review*, 34, 582-594. Disponible en: https://doi.org/10.1016/j.clsr.2017.12.001.

Ni Loidean, N. (2016). The end of Safe Harbor: implications for EU Digital Privacy and Data Protection Law. *Internet Law Journal*, 19 (8), 1-8.

Ortega Giménez, A. (2017). Transferencia internacional de datos personales: del Safe Harbour al Privacy Shield. *Revista Lex Mercatoria*, 4, 85-90. Disponible en: https://doi.org/10.21134/lex.v2i3.1093.

Ortega Giménez, A. (2019). El impacto del Reglamento General de Protección de Datos de la Unión Europea y de la LOPDGDD en el régimen jurídico de las transferencias internacionales de datos de carácter personal. En R. García Mahamut y B. Tomás Mallén (eds.). *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de datos y garantía de los derechos digitales* (pp. 393-417). Valencia: Tirant lo Blanch.

Otero García-Castrillón, C. (2020). The CJEU Shrems cases – Personal Data Protection and International Trade Regulation. *Conflict of Laws.net*, 19-12-2020. Disponible en: https://bit.ly/3kNEi17.

Piñar Mañas, J. L. (2016). Transferencias de datos personales a terceros países u organizaciones internacionales. En M. Álvarez Caro, M. Recio Gayo y J. L. Piñar Mañas (eds). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad* (pp. 431-464). Madrid: Reus.

Recio Gayo, M. (2019). Nivel adecuado para transferencias internacionales de datos. *Revista de Derecho Pontificia Universidad Católica del Perú*, 83, 207-240. Disponible en: https://doi.org/10.18800/derechopucp.201902.007.

Roth, P. (2017). Adequate level of data protection in third countries post-Schrems and under the General Data Protection Regulation. *Journal of Law, Information and Science*, 25 (1), 49-60.

Ruiz Tarrías, S. (2020). 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, 11-162. Disponible en: https://doi.org/10.37417/REDE/num76_2020_532.

Schwartz, P. M. (2009). Managing Global Data Privacy: Cross-Border information flows in a networked environment. *The Privacy Projects*. Disponible en: https://bit.ly/3gflogB.

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

Sobrino García, I. (2019). Protección de datos y privacidad. Estudio comparado del concepto y su desarrollo entre la Unión Europea y Estados Unidos. *Revista de Derecho de la Universidad Nacional de Educación a Distancia*, 25, 687-713. Disponible en: https://doi.org/10.5944/rduned.25.2019.27017.

Sobrino García, I. (2020). La invalidez del Privacy Shield y la supervivencia de las cláusulas contractuales tipo. *LA LEY Unión Europea*, 84, 1-10.

Sobrino García, I. (2021). Desafíos y limitaciones en la contratación pública: el impacto de la protección de datos tras los últimos cambios legislativos. *Revista General de Derecho Administrativo*, 56, 1-34.

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

Tracol, X. (2016). Invalidator Strikes Back: the Harbor has Never Been Safe. *Computer Law and Security Review,* 32 (2), 345-362. Disponible en: https://doi.org/10.1016/j.clsr.2016.01.011.

Wagner, J. (2018). The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection? *International Data Privacy Law*, 8 (4), 318-337. Disponible en: https://doi.org/10.1093/idpl/ipy008.