ISSN: 2697-1631 | ISSN-e: 2697-2239

Las sentencias Schrems I (2015) y Schrems II (2020) del Tribunal de Justicia de la Unión Europea y la protección de datos de carácter personal en las relaciones internacionales

Nicolás Cabezudo Vidal

Capital markets legal trainee. Ramon y Cajal Abogados (España)

nicabe99@gmail.com | https://orcid.org/0000-0002-4729-0469

Extracto

El objeto principal de este trabajo se centra en el análisis de las garantías y mecanismos de protección del derecho fundamental a la protección de datos de carácter personal en el ámbito de las transferencias internacionales de datos que se producen entre un Estado de la Unión Europea y un tercer Estado, lo que llevará, entre otros extremos, al análisis de las sentencias del Tribunal de Justicia de la Unión Europea Schrems I, de 15 de julio de 2015, y Schrems II, de 16 de julio de 2020, dos casos paradigmáticos que suponen un importante avance en la doctrina del Tribunal de Justicia de la Unión relativa al derecho a la protección de datos de carácter personal y que nos ofrecen una interesante información acerca de la dificultad de fijar medidas de protección eficaces cuando los datos personales traspasan las fronteras de la Unión.

Palabras clave: Schrems; datos personales; transferencias internacionales de datos; *safe harbour*; *privacy shield*.

Recibido: 04-05-2022 / Aceptado: 27-09-2022 / Publicado: 10-02-2023

Cómo citar: Cabezudo Vidal, N. (2023). Las sentencias Schrems I (2015) y Schrems II (2020) del Tribunal de Justicia de la Unión Europea y la protección de datos de carácter personal en las relaciones internacionales. *CEFLegal. Revista Práctica de Derecho*, *265*, 91-126. https://doi.org/10.51302/ceflegal.2023.15785

The Schrems I (2015) and Schrems II (2020) judgments of the Court of Justice of the European Union and the personal data protection in international relations

Nicolás Cabezudo Vidal

Abstract

The main purpose of this paper is to analise the guarantees and mechanisms of protection of the fundamental right to personal data protection in the field of international data transfers that occur between a State of the European Union and a third State, which will lead, among other things, to the analysis of the judgments of the Court of Justice of the European Union Schrems I, of July 15, 2015, and Schrems II, of July 16, 2020, two paradigmatic cases that represent an important advance in the doctrine of the Court of Justice of the Union regarding the right to personal data protection and that offer us interesting information about the difficulty of establishing effective protection measures when personal data cross the borders of the Union.

Palabras clave: Schrems; personal data; international data transfers; safe harbour; privacy shield.

Received: 04-05-2022 / Accepted: 27-09-2022 / Published: 10-02-2023

Citation: Cabezudo Vidal, N. (2023). Las sentencias Schrems I (2015) y Schrems II (2020) del Tribunal de Justicia de la Unión Europea y la protección de datos de carácter personal en las relaciones internacionales. *CEFLegal. Revista Práctica de Derecho*, *265*, 91-126. https://doi.org/10.51302/ceflegal.2023.15785

Sumario

Nota: Este trabajo tiene su origen en las investigaciones que el autor comenzó en el marco de las actividades de una beca de colaboración en el área de Derecho Constitucional de la facultad de Derecho de la Universidad de Valladolid, durante el curso 2020-2021, y que se plasmaron en el trabajo de fin de grado, dirigido por el profesor Juan Fernando Durán Alba, defendido como conclusión de sus estudios, que obtuvo la máxima calificación (accesible en https://uvadoc.uva.es/bitstream/handle/10324/51199/TFG-D_01281.pdf?isAllowed=y&sequence=1). El presente texto desarrolla y precisa algunos aspectos abordados en dicho trabajo.

1. Introducción[1]

La complejidad técnica, cada vez más sofisticada, de lo que se ha venido a calificar como «tecnologías disruptivas»[2], junto al fenómeno de la globalización, plantean importantes retos en relación con la protección de datos de carácter personal. Por un lado, los avances tecnológicos permiten que tanto las empresas privadas como las autoridades públicas realicen operaciones de tratamiento de datos personales, como la recogida, registro, conservación o difusión, en una escala cuantitativa sin precedentes, y por otro, la integración de la economía en un mercado global, con una continua movilización de bienes y servicios, de capital y de trabajadores fuera de las fronteras nacionales, unido a la proliferación de las redes de comunicación social en sitios web o mediante aplicaciones[3], conlleva una continua circulación de datos personales más allá de las fronteras del propio Estado.

Este continuo flujo transfronterizo de datos personales hace que sea muy complicado establecer mecanismos jurídicos que protejan a las personas frente al tratamiento no autorizado de sus datos de carácter personal, pues el mundo digital carece de fronteras geográficas, los distintos Estados cuentan con muy diversos estándares de protección de los

[1] Valga esta primera nota para manifestar mi agradecimiento a mi amigo y profesor de Derecho Constitucional Juan Fernando Durán Alba por su constante ayuda y apoyo tanto en la elaboración de este trabajo como en el desarrollo de mi formación universitaria.

[2] Se utiliza el adjetivo «disruptivas» para calificar a las nuevas tecnologías que se caracterizan por una radical innovación que deja obsoleta la tecnología anterior. Son ejemplos claros el *big data*, la inteligencia artificial, la prestación de servicios de *cloud computing* o la tecnología *blockchain*, entre otras.

[3] Facebook y Twitter, por ejemplo, pero hay otras destinadas a compartir contenido audiovisual (YouTube, Snapchat, Instagram), a facilitar contactos laborales (Linkedin), a promover el social *blogging* (Medium, Tumblr) o a fomentar debates (Reddit, Quora).

datos de carácter personal y los prestadores de bienes o servicios *online* pueden fijar su sede en cualquier lugar físico, por lo que ostentan una posición dominante en el mercado frente a los ciudadanos, que se encuentran en una clara situación de inferioridad.

Por todo ello, tal y como se intentará argumentar a lo largo de las siguientes líneas, la Unión Europea ha asumido, desde hace décadas, una importante labor en la articulación de instrumentos jurídicos dirigidos a garantizar un nivel elevado de protección de los datos personales de los ciudadanos comunitarios, no solo dentro de la Unión, sino también cuando los datos personales se transfieren a un tercer Estado como consecuencia de operaciones comerciales o de otra naturaleza. En esta última situación se exigirá que el país receptor garantice un nivel de protección sustancialmente equivalente al existente en la Unión Europea.

Pues bien, el objeto principal de este trabajo se centra en el análisis de las garantías y mecanismos de protección del derecho fundamental a la protección de datos de carácter personal en el ámbito de las transferencias internacionales de datos que se producen entre un Estado de la Unión Europea y un tercer Estado, lo que llevará, entre otros extremos, al análisis de las sentencias del Tribunal de Justicia de la Unión Europea Schrems I, de 15 de julio de 2015 (Gran Sala)[4], y Schrems II, de 16 de julio de 2020 (Gran Sala)[5], dos casos paradigmáticos que suponen un importante avance en la doctrina del Tribunal de Justicia de la Unión Europea (TJUE) relativa al derecho a la protección de datos de carácter personal y que nos ofrecen una interesante información acerca de la dificultad de fijar medidas de protección eficaces cuando los datos personales traspasan las fronteras de la Unión.

En el marco de lo expuesto anteriormente, una idea general atraviesa transversalmente este trabajo, y es que no se puede entender el derecho, las normas jurídicas, al margen de los hechos, de los fenómenos sociales o de los avances tecnológicos. Por ello, solo a partir de un conocimiento realista de los casos en que la tecnología invade y limita nuestros derechos fundamentales es posible articular mecanismos jurídicos para hacer frente a las amenazas que emanan de un mundo digital sin fronteras físicas. Pero junto a esta consideración, las reglas que rigen las relaciones comerciales privadas, muchas de ellas vinculadas al principio de la autonomía de la voluntad, ponen énfasis en la necesidad de que los datos de carácter personal fluyan sin cortapisas fuera de las fronteras nacionales, porque, caso contrario, se pone en peligro la integración de la economía nacional o europea en un mercado global, con una continua movilidad de bienes, de servicios, de capital, de trabajadores y, necesariamente, de datos de carácter personal.

En esta encrucijada se encuentra tanto el derecho constitucional, cuyo ámbito de protección y control natural se ciñe a las fronteras del Estado respecto del que proyecta sus

[4] Sentencia de 6 de octubre de 2015, Schrems (C-362/14, EU:C:2015:650).

[5] Sentencia de 16 de julio de 2020, Schrems (C-311/18, EU:C:2020:559).

efectos la Constitución normativa, como el derecho de la Unión Europea, desde el que se está realizado un elogiable esfuerzo con la finalidad de articular instrumentos jurídicos dirigidos a garantizar el derecho fundamental a la protección de datos de carácter personal de los ciudadanos comunitarios, no solo dentro de la Unión, sino también *ad extra*, exigiendo que terceros países con los que se realice cualquier tipo de transferencia de datos personales, ya sea en el ámbito público o en el privado, garanticen un nivel de protección sustancialmente equivalente al prestado dentro del territorio comunitario y, caso contrario, prohibiendo la transferencia de datos a dichos países.

La pregunta es obligada: ¿puede la Unión Europea intervenir en las relaciones comerciales con terceros Estados hasta el extremo de prohibirlas cuando no es posible asegurar la protección de los datos de carácter personal de los usuarios de esos servicios? La respuesta nos reconduce a los *leading cases*, que constituyen el núcleo principal de este trabajo: las STJUE Schrems I y II del TJUE. No obstante, el punto de arranque de nuestra investigación lo podemos situar en junio del año 2013, cuando el señor Edward Snowden, un joven informático norteamericano que trabajaba para la NSA (National Security Agency, de los Estados Unidos) filtró a la prensa diversos documentos calificados «de alto secreto», que revelaban la existencia de varios programas de vigilancia estatal masiva, como PRISM o Upstream. Estas revelaciones contemplaban la recogida y tratamiento a gran escala de datos personales de ciudadanos norteamericanos y de terceros países, entre los que se encontraban, como no podía ser de otra manera, ciudadanos europeos.

Estas filtraciones rompieron la relación de confianza con los Estados Unidos en lo que respecta a la protección de los datos personales de los ciudadanos comunitarios y dieron lugar a un tsunami de críticas dirigidas a las autoridades estadounidenses. Sin embargo, la Comisión Europea no suspendió, como hubiera sido procedente, la «decisión de adecuación del año 2000», que declaraba que Norteamérica era un «puerto seguro» para los datos personales de los ciudadanos comunitarios, cuestión sobre la que volveremos más adelante. Ahora bien, frente a la pasividad de la Comisión Europea, será otro particular, el señor Schrems, quien decidió emprender una lucha personal digna de ser comparada con la batalla entre David y Goliat, iniciando una contienda judicial contra la empresa norteamericana Facebook Inc., red social de la que era usuario y cuya filial en Europa tiene sede en Irlanda, denunciando ante la autoridad de protección de datos irlandesa que dicha empresa no garantizaba la seguridad de sus datos personales frente a una eventual intervención de las autoridades norteamericanas amparada en presuntas razones de seguridad nacional.

Como se explicará a lo largo de las siguientes líneas, el caso llegó al TJUE y la Gran Sala dictó sentencia, de fecha 6 de octubre de 2015, anulando la citada decisión de adecuación de la Comisión Europea. Dicho de otro modo: el TJUE le grita al mundo que los Estados Unidos no son un «puerto de destino seguro» para los datos personales de los ciudadanos de la Unión Europea y, por extensión, para ninguna persona, sea cual fuere su nacionalidad. Las consecuencias de esta sentencia fueron muy serias: pérdida de fiabili-

dad de las decisiones de adecuación de la Comisión Europea, inexistencia de garantías de protección de los datos personales en las relaciones comerciales con los Estados Unidos e incertidumbre para las empresas, al ponerse en peligro la fluidez de las relaciones comerciales con dicho país.

Todo ello va a forzar, en el año 2016, una segunda decisión de adecuación de la Comisión, que lleva aparejado el calificado como «acuerdo del escudo de privacidad», con el ingenuo planteamiento de que los Estados Unidos han reforzado su sistema de garantías para una efectiva protección de los datos personales de los ciudadanos comunitarios. Sin embargo, la historia se repite, Schrems vuelve a acudir a los tribunales irlandeses y el caso llega de nuevo al TJUE, que anula la segunda decisión de adecuación de la Comisión respecto de los Estados Unidos y reitera su doctrina respecto de lo que son los estándares europeos de protección de datos personales. Cuestiones, todas ellas, sobre las que se pretende profundizar a lo largo de las siguientes páginas.

2. La protección de los datos de carácter personal como derecho fundamental en el ámbito de la Unión Europea

Seguramente es ocioso recordar que el Tratado de Lisboa, firmado el 13 de diciembre de 2007 por los Estados miembros de la Unión Europea[6], constituye un paso definitivo en el «prolongado esfuerzo por revestir la construcción europea de dimensión constitucional» (López Aguilar, 2017, p. 557), no solo porque incorpora al Tratado de la Unión Europea (en adelante, TUE) preceptos que aseguran la fuerza vinculante de los principios generales y de las tradiciones constitucionales comunes de los Estados miembros como fuente del derecho europeo (arts. 2, 3, 4 y 6 TUE), sino también porque, tras su firma, la Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000 (CDFUE)[7], que pasará a tener el mismo valor jurídico que los tratados, tal y como prevé el artículo 6 del TUE. Asimismo, la Unión reconoce que los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales formarán parte del derecho de la Unión como principios generales (art. 6.3 TUE)[8] y, como ha tenido ocasión de

[6] Denominado formalmente «Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea», entró en vigor el 1 de diciembre de 2009.

[7] Proclamada por el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea el 7 de diciembre de 2000 en Niza. Una versión revisada de la Carta fue proclamada y firmada el 12 de diciembre de 2007 en Estrasburgo por los mismos órganos.

[8] Para una mayor profundización sobre esta cuestión puede consultarse, entre otros muchos: Balaguer Callejón (2008) y Carmona Contreras (2016).

declarar el TJUE, aunque los derechos contenidos en la Carta se correspondan con derechos garantizados por el Convenio Europeo de Derechos Humanos, este no constituye un instrumento jurídico integrado formalmente en el ordenamiento jurídico de la Unión, toda vez que la Unión aún no se ha adherido formalmente a él[9].

A los efectos de este trabajo, nos interesa reparar en algo ya plenamente asumido, como es la importancia de la incorporación de la CDFUE de la Unión Europea como derecho vinculante, tanto para las instituciones, órganos y organismos de la Unión, como para los Estados miembros cuando apliquen el derecho de la Unión[10], así como en la transcendental labor del TJUE en la defensa de estos derechos y en la delimitación de su contenido y garantías. En este sentido, los estudios más recientes de la doctrina especializada señalan al menos tres ámbitos específicos de incidencia decisiva de la jurisprudencia del Tribunal de Justicia sobre la de los tribunales garantes de los ordenamientos de los Estados miembros: el acceso a la justicia y a la tutela judicial; la igualdad de trato y no discriminación; y, en lo que ahora nos ocupa, la privacidad, la vida privada y la protección de datos[11].

Centrándonos en el último de los ámbitos señalados, el artículo 7 de la CDFUE establece que «toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones», y el artículo 8. 1 de la CDFUE reconoce a toda persona «el derecho a la protección de los datos de carácter personal que le conciernan», lo que ha de completarse con lo previsto en el apartado segundo de ese mismo artículo, en el que se recoge que los datos de carácter personal «se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley». El artículo 8 de la CDFUE se cierra con un tercer apartado, en el que se indica que «el respeto de estas normas estará sujeto al control de una autoridad independiente».

Más allá de los artículos reproducidos, la Carta no ofrece una definición detallada de este derecho, pero, como se desprende de la jurisprudencia del TJUE y de las normas comunitarias dirigidas a proteger el derecho a la protección de datos personales, en el ámbito de la Unión Europea el valor o bien jurídico protegido por este derecho fundamental es la libertad del individuo frente a los abusos y presiones a los que puede verse sometido, por poderes públicos o por particulares, como consecuencia del acceso y tratamiento de sus

[9] SSTJUE de 26 de febrero de 2013, Akerberg Fransson (C617/10, EU: C:2013:105), apartado 44 y jurisprudencia citada, y de 20 de marzo de 2018, Menci (C524/15, EU:C:2018:197), apartado 22.

[10] Para Mangas Martín (2008, p. 814) «parece inevitable que la Carta penetre en la totalidad de la actividad normativa y ejecutiva del Estado», de tal manera que los ciudadanos pueden invocar «los derechos reconocidos en la Carta ante los jueces sin distingos de si la efectividad interna es competencia propia o competencia atribuida».

[11] Sobre el importante papel del TJUE en la defensa de los derechos de la Carta puede consultarse Saiz Arnaiz (2005).

datos personales, que no son solo aquellos que pueden calificarse como íntimos, sino toda información relativa a una persona física identificada o identificable[12].

Asimismo, no se ha de olvidar que, conforme al artículo 52.1 de la CDFUE, cualquier limitación del ejercicio de los derechos y libertades reconocidos por la Carta deberá estar prevista en la ley y respetar su contenido, lo que ha de completarse con lo recogido en el artículo 52.1 de la CDFUE, en el que se indica que, atendiendo al principio de proporcionalidad, solo podrán introducirse limitaciones a dichos derechos y libertades cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de otros derechos y libertades reconocidos en la Carta, lo que, trasladado a la protección de datos de carácter personal, ha llevado al TJUE a sostener que para cumplir el principio de proporcionalidad, los posibles límites a la protección de los datos personales «no deben exceder de lo estrictamente necesario», insistiendo en que «la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso»[13]. En particular, dicha normativa 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[14].

Por ello, la jurisprudencia del TJUE dictada en materia de protección de datos ha tenido una influencia decisiva para la configuración del contenido de este derecho por parte de los tribunales constitucionales de los Estados miembros, siendo interesante resaltar desde estas líneas que el TJUE siempre se ha mostrado especialmente severo a la hora de exigir que la Unión Europea garantice unos estándares de protección rigurosos en la protección de los datos personales, no solo dentro de las fronteras de la Unión, sino también respecto de terceros países. También es importante aclarar que, de acuerdo con una reiterada jurisprudencia, dada la ausencia en el derecho de la Unión de una remisión expresa al derecho nacional de los Estados miembros, la interpretación de los derechos de la Carta no se realiza a la luz del derecho nacional, aunque sea de rango constitucional[15], incluso en aquellos supuestos en los que los Estados miembros mantengan unos altos estándares de protección, como es el caso de la jurisprudencia del Tribunal Constitucional de España, que ha tenido un papel muy importante en la configuración del derecho fundamental a la protección de

[12] Como recogía, con anterioridad a la entrada en vigor de la Carta, la Directiva 95/46/CE, en su artículo 2 a).

[13] Así lo indica en el apartado 176 de la sentencia Schrems II, que analizaremos con detenimiento más adelante.

[14] Véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UECanadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada.

[15] Como se indica en la STJUE de 18 de octubre de 2016, Nikiforidis (C135/15, EU:C:2016:774), apartado 28.

datos de carácter personal como derecho fundamental, con un contenido autónomo, distinto al derecho a la intimidad, pudiendo destacar las SSTC 290/2000 y 292/2000, ambas de 30 de noviembre, dado que son las primeras que reconoce un derecho fundamental *ex novo* a la protección de datos de carácter personal a partir del artículo 18.4 de la CE[16], sin perjuicio de que hay otras sentencias previas, como la STC 254/1993, de 20 de julio, en la que el Tribunal Constitucional ya indica que del artículo 18.4 de la CE se desprende un instituto de garantía de los derechos a la intimidad y al honor que es, además, en sí mismo, «un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos» (FJ 6)[17].

3. La normativa europea dirigida a la protección de los datos personales en las transferencias internacionales de datos

Desde estas líneas no se pretende llevar a cabo un análisis pormenorizado de la normativa de la Unión Europea en materia de protección de datos, sino solo examinar la regulación que está directamente relacionada con las transferencias de datos personales desde la Unión Europea a terceros países o a organizaciones internacionales, en especial cuando la transferencia se produce como consecuencia de las relaciones comerciales entre dos o más operadores jurídicos. Pues bien, desde un punto de vista cronológico, el primer instrumento jurídico relevante se materializa en la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, 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[18], que nace para hacer frente a todos los problemas derivados de la legislación divergente entre los Estados miembros de la UE en materia de protección de datos y que estuvo vigente hasta la entrada en vigor del actual 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 su libre circulación.

En lo que ahora nos interesa, la directiva preveía que las transferencias de datos personales a un tercer país que no garantizase un nivel de protección adecuado solo podrían realizarse cuando el responsable del tratamiento ofreciera garantías suficientes dirigidas a asegurar la vida privada y el resto de derechos y libertades fundamentales que pudieran

[16] Que dispone: «Se limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

[17] Sobre esta materia puede consultarse, entre otros, Aguado Renedo (2010). Más recientemente Bilbao Ubillos (2020, pp. 66 y ss.).

[18] La Directiva 95/46/CE fue transpuesta en España en diciembre de 1999, mediante la Ley Orgánica 15/1999 de protección de datos (LOPD), que entró en vigor en enero del 2000.

verse afectados. Dichas garantías podían derivarse «de cláusulas contractuales apropiadas», que deberían controlarse a través de las autoridades de control de la protección de datos de carácter personal existentes en los Estados miembros, siendo abundante la jurisprudencia del TJUE que pone especial énfasis en su importancia[19].

Siguiendo una exposición cronológica de los principales instrumentos jurídicos de la Unión Europea en relación con la protección de datos objeto de las transferencias a terceros países, debemos llamar la atención sobre diversas decisiones de la Comisión[20], comenzando con la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, conocida coloquialmente como «acuerdo de puerto seguro», que constituye una de las denominadas «decisiones de adecuación» a las que se refiere la directiva[21], en este caso con la finalidad de fijar las condiciones de protección de los datos de carácter personal en las transferencias de datos entre la Unión Europea y los Estados Unidos de Norteamérica, que constituye el objeto de impugnación de la STJUE Schrems I.

Adelantamos que se trata de una decisión de adecuación parcial, es decir, su mera aprobación no supone la presunción de adecuación de la totalidad de las empresas estadounidenses, sino que únicamente afectará a aquellas que formen parte del acuerdo y, por lo tanto, solo servirá de cobertura legal a las empresas norteamericanas que se comprometan a cumplir todos los principios recogidos en el mismo, pero, en todo caso, resulta un caso paradigmático que pone de relieve algunos de los problemas que surgen con terceros países (no necesariamente del tercer mundo) cuando se trata de proteger los datos de carácter personal que se transfieren desde la Unión Europea.

También destaca la Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a las «cláusulas contractuales tipo para la transferencia de datos personales a un tercer país», en la que se define las «cláusulas contractuales tipo» como un instrumento idóneo para garantizar un nivel adecuado de protección de los datos personales transferidos de la UE a

19 SSTJUE de 9 de marzo de 2010, Comisión/Alemania (C518/07, EU:C:2010:125), apartado 25 y de 8 de abril de 2014, Comisión/Hungría (C288/12, EU:C:2014:237), apartado 48 y la jurisprudencia citada. Para garantizar esa protección, las autoridades nacionales de control han de lograr un justo equilibrio entre el respeto del derecho fundamental a la vida privada y los intereses que exigen la libre circulación de datos personales (véanse, en ese sentido, las STJUE citadas, en sus apartados 24 y 51, respectivamente).

20 De acuerdo con lo dispuesto en los artículos 288 y siguientes del TFUE, la decisión vincula de manera directa e inmediata a sus destinatarios en todos sus elementos. Una decisión puede dirigirse a las instituciones, órganos, organismos y funcionarios de la Unión, a uno o varios de sus Estados miembros, o a particulares.

21 El artículo 25.6 de la directiva disponía: La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5.

terceros países y que fue modificada pocos años después por la Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004, mediante la introducción de un conjunto alternativo de cláusulas contractuales para la transferencia de datos personales a terceros países. Unos años más tarde, todas las decisiones anteriores se sustituyen por la Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, también relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, que forma parte del objeto de análisis de la STJUE Schrems II, así como la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, sobre la adecuación de la protección conferida por el Escudo de privacidad entre la Unión Europea y los Estados Unidos, sobre las que también volveremos más adelante.

Finalmente, el 14 de abril de 2016, tras un largo proceso legislativo, se aprobó el 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 (RGPD), que establece nuevas reglas y sustituye el marco regulador anteriormente descrito. Su aplicación directa a los diferentes Estados miembros, sin necesidad de trasposición por las normas nacionales, ha permitido la armonización de la protección de datos en todos los Estados miembros de la Unión Europea[22].

En el considerando número 101, el reglamento hace una primera referencia a los flujos transfronterizos de datos personales a países y organizaciones internacionales no pertenecientes a la Unión, constatando que dicha transferencia de datos es necesaria «para la expansión del comercio y la cooperación internacionales», pero también insistiendo en que si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países, «esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento». En este sentido, en el considerando 103 el reglamento adelanta el importante papel que se le otorga a la Comisión, pues será el órgano encargado de decidir, con efectos para toda la Unión, que un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional, ofrecen un nivel de protección adecuado de los datos de carácter personal transferidos desde la Unión, aportando de esta forma seguridad y uniformidad jurídica a toda la Unión. Todo ello se regula de manera pormenorizada en el capítulo V del RGPD, que se dedica a la «transferencias de datos personales a terceros países u organizaciones internacionales» (arts. 44 al 50), que, por razones sistemáticas, analizaremos con detenimiento más adelante.

[22] Pese a la aplicación directa del Reglamento general de protección de datos de la Unión Europea, que comenzó a aplicarse en España a partir del 25 de mayo de 2018, fue necesaria la elaboración de una nueva ley orgánica en España, que se concretó en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

4. Las transferencias de datos de carácter personal entre Europa y Estados Unidos

4.1. El «acuerdo de puerto seguro» (*safe harbour*) recogido en la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000

Como ya hemos adelantado, la Decisión 2000/520/CE, de 26 de julio de 2000, fue adoptada por la Comisión con apoyo en el artículo 25.6 de la Directiva 95/46/CE[23], con la finalidad de establecer un nivel adecuado de protección de los datos de carácter personal en las transferencias desde la Unión Europea a los Estados Unidos de América.

Para entender la importancia de esta decisión, hay que tener en cuenta que la aprobación de la Directiva 95/46/CE provocó cierta preocupación entre las empresas europeas y norteamericanas, pues se temía que las duras exigencias de protección de datos exigidas por la Unión Europea afectaran negativamente a las relaciones comerciales entre ambos países, dado que la legislación norteamericana resultaba (y resulta) mucho más laxa que la europea, pues se apoya en un sistema de «autorregulación» entre las empresas y los interesado, mientras que en Europa se parte de una legislación general directamente vinculante para poderes públicos y particulares. Esta situación llevó al Departamento de Comercio de Estados Unidos a iniciar en 1998 negociaciones con la Comisión Europea, con la finalidad de establecer unos estándares de protección adecuados que facilitaran el flujo de datos personales entre la Unión Europea y los Estados Unidos de Norteamérica[24].

Desde la entrada en vigor de esta decisión, el 26 de julio de 2000, hasta el 6 de octubre de 2015, fecha en que el TSJUE anuló dicha norma comunitaria mediante la sentencia Schrems I, las transferencias internacionales de datos realizadas entre la Unión Europea y los Estados Unidos estaban basadas en el llamado «acuerdo de puerto seguro» (*safe harbour*), regulado en la citada decisión, de tal manera que todas aquella empresas norteamericanas suscritas a dicho acuerdo asumían el cumplimiento de la normativa europea relativa a la protección de datos de carácter personal, evitando así la necesidad de un control individualizado de todas las transferencias de datos realizadas entre cualquiera de los países de la Unión y las empresas.

---

[23] El artículo 25.2 establecía: «El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países».

[24] Algunos documentos relevantes relativos a dichas negociaciones pueden encontrarse en: http://export.gov/safeharbor/eu/eg_main_018496.asp

En síntesis, la Decisión 2000/520/CE, de 26 de julio de 2000, establecía que el nivel adecuado de protección de la transferencia de datos desde la Unión Europea a los Estados Unidos de América solo podría alcanzarse si las entidades y empresas norteamericanas cumplían un conjunto de requisitos calificados como «principios de puerto seguro» (recogidos en el anexo I de la decisión). Asimismo, se recogía un elenco de preguntas y respuestas englobadas bajo las siglas FAQ (*frequently answers and questions*), a través de las que se proporcionaba orientación para aplicar los referidos principios. Por su parte, las entidades y empresas norteamericanas debían dar a conocer públicamente sus políticas de protección de los datos de carácter personal y someterse a la jurisdicción de la Comisión Federal de Comercio (Federal Trade Commission), que prohíbe actos o prácticas desleales o fraudulentas en el comercio o en relación con él.

Hay que recordar, como ya advertimos, que estamos ante una decisión de adecuación parcial, por lo que su mera aprobación no suponía la presunción de adecuación de la totalidad de las empresas estadounidenses, sino que únicamente afectaba a aquellas que suscribían el «acuerdo de puerto seguro» y que, en consecuencia, se comprometían a cumplir los principios que se derivaban del mismo. Con esta finalidad, las empresas que se quería adherir a este sistema de protección debían presentar una «carta de autocertificación» ante el Departamento de Comercio de los Estados Unidos, a través de la que manifestaban su adhesión. ¿De qué modo una entidad «autocertificaba» su adhesión a los «principios de puerto seguro»? Se trata de una pregunta frecuente (FAQ), por lo que en el anexo II de la decisión se explicaba que para proceder a la autocertificación las entidades podían proporcionar al Departamento de Comercio una carta firmada por uno de los responsables de la empresa en nombre de la entidad, declarando su adhesión al «acuerdo de puerto seguro».

Por lo demás, las empresas norteamericanas que suscribían el «acuerdo de puerto seguro» estaban sujetas a la jurisdicción de uno de los organismos públicos estadounidenses que figuraban en el anexo VII de la decisión, facultados para investigar las quejas que pudieran presentarse y para solicitar medidas provisionales contra las prácticas desleales o fraudulentas, así como para establecer las reparaciones que fuesen necesarias para los particulares perjudicados, independientemente de su país de residencia o de su nacionalidad.

En el anexo I de la decisión se recogen los «principios de puerto seguro», que pueden resumirse en los siguientes puntos: a) principio de notificación (*notice*): establece la obligación que tienen las entidades y empresas de informar a los interesados de los fines y tratamiento de sus datos de carácter personal; b) principio de opción (*choice*): dispone la obligación de las entidades y empresas de ofrecer a los particulares la posibilidad de decidir si sus datos de carácter personal pueden ser o no cedidos a un tercero; c) principio de transferencia ulterior (*onward transfer*): señala que para revelar información a terceros que no participen en el «acuerdo de puerto seguro», las entidades y empresas deberán

aplicar los principios de notificación y de opción; d) principio de seguridad (*security*): dispone que las entidades y empresas que se encarguen de la recogida de datos de carácter personal deberán tomar todas las precauciones que estimen oportunas con el fin de evitar la pérdida, modificación o destrucción de los mismos; e) principio de integridad de los datos (*data integrity*): señala que los datos de carácter personal deben ser pertinentes con respecto a los fines para los que se recaban; f) principio de acceso (*access*): recoge el derecho de los particulares a conocer aquellos datos de carácter personal que las entidades tengan sobre ellos y el derecho a poder corregirlos, modificarlos o suprimirlos en caso de que sean inexactos; g) principio de aplicación (*enforcement*): fija la necesidad de incluir una vía de recurso para los interesados que se vean afectados por el incumplimiento de la normativa sobre la transferencia internacional de datos de carácter personal entre los Estados Unidos y la Unión Europea.

De acuerdo con lo expuesto, todo parecía indicar que la Decisión 2000/520/CE garantizaba que los Estados Unidos era un Estado seguro respecto de las garantías de protección de los datos personales de los ciudadanos europeos. Sin embargo, como veremos a continuación, los principios generales antes expuestos cedían en aquellos supuestos en que las autoridades norteamericanas invocasen genéricas razones de «seguridad nacional», sin que la normativa de los Estados Unidos previese recurso alguno ante ningún órgano judicial para impugnar la proporcionalidad de dicha intervención estatal. Dicho de otro modo, los «principios de puerto seguro» eran solo aplicables a particulares y empresas estadounidenses que se hubiesen adherido a él, pero las autoridades públicas norteamericanas no estaban sometidas a dicho régimen, prevaleciendo las exigencias de seguridad nacional, interés público y cumplimiento de la ley de los Estados Unidos, lo que estaba previsto en el anexo I de la Decisión 2000/520/CE.

4.2. Cuando la vulneración del derecho a la protección de los datos personales no procede de los particulares, sino de las autoridades públicas norteamericanas

Como se recordará, pues la prensa nacional e internacional dio buena cuenta de la noticia, en junio de 2013 el Sr. Edward Snowden, un joven informático norteamericano que trabajaba para la Agencia de Seguridad Nacional de los Estados Unidos (NSA), descubrió e hizo pública la vigilancia ejercida por el Ejecutivo de los Estados Unidos sobre ciudadanos norteamericanos y de terceros países, quien, sin autorización judicial e invocando genéricos «intereses relacionados con la seguridad nacional», interceptaba teléfonos y correos electrónicos, accedía a datos de carácter personal de ficheros de empresas (como Facebook), sustraía información a gobiernos de terceros Estados, etc. La denuncia pública contaba con pruebas fehacientes, pues Snowden filtró a la prensa un importante número de documentos calificados como «de alto secreto», que evidenciaban la ilegítima conducta de la potencia americana en la privacidad de la población mundial.

De las revelaciones hechas por Edward Snowden respecto de la existencia en los Estados Unidos de varios programas de vigilancia estatal (como el programa PRISM, que comprendían la recogida y el tratamiento a gran escala de datos personales de ciudadanos norteamericanos y de personas de terceros países), la Comisión Europea se vio en la necesidad de aprobar, el 27 de noviembre de 2013, la Comunicación al Parlamento Europeo y al Consejo titulada «Restablecer la confianza en los flujos de datos entre la UE y EE. UU.»[25], que iba acompañada de un informe sobre protección de datos personales, también con fecha de 27 de noviembre de 2013, elaborado por un grupo de trabajo creado *ad hoc* y formado por representantes de la Unión Europea y de los Estados Unidos de Norteamérica (*Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection*), que contenía un exhaustivo estudio del ordenamiento jurídico de los Estados Unidos de América en lo que se refiere a la regulación legal que autoriza la existencia de programas de vigilancia y de recogida y tratamiento de datos personales por el Gobierno estadounidense, que hay que poner en conexión con lo dispuesto en el punto 2 de la citada comunicación al Parlamento Europeo y al Consejo, en la que la Comisión manifestaba que «ha aumentado la preocupación por el nivel de protección de los datos personales de los ciudadanos de la [Unión] transferidos a Estados Unidos en el marco del régimen de Puerto Seguro», y con el punto 3.2, en el que se constatan serias deficiencias en la aplicación de la Decisión 2000/520/CE, concluyendo que «habida cuenta de las deficiencias halladas, no puede mantenerse la aplicación actual del régimen de Puerto Seguro», pero añadiendo que, toda vez que su derogación afectaría negativamente a los intereses de las empresas de la Unión Europea y de los Estados Unidos que se han adherido al mismo, la Comisión, con carácter de urgencia, «debatirá con las autoridades de Estados Unidos las deficiencias detectadas» con la finalidad de llegar a una solución[26].

La Comisión no utiliza términos diplomáticos cuando acusa directamente a las autoridades norteamericanas de no aplicar los principios de legalidad, necesidad y proporcionalidad, pues afirma que, al tratarse de programas a gran escala y sin intervención judicial «puede ocurrir que las autoridades estadounidenses accedan y procesen los datos transferidos al amparo del puerto seguro más allá de lo estrictamente necesario y proporcionado para la protección de la seguridad nacional, como reza la excepción prevista en la Decisión [2000/520/CE]»; a lo que se une, como se indica en el punto 7.2, que las garantías de protección previstas por la legislación estadounidense se refieren a los ciudadanos estadounidenses o a los residentes legales, sin que esté prevista la posibilidad de que los ciudadanos de la Unión Europea puedan acceder a sus datos, rectificarlos o suprimirlos, ni obtener reparación administrativa o judicial, cuando dichos datos son re-

[25] COM (2013) 846 final.

[26] Como se desprende de la comunicación que analizamos, a 26 de septiembre de 2013 se habían adherido al «acuerdo de puerto seguro» un total de 3.246 entidades privadas pertenecientes a sectores de la industria y al sector servicios.

cogidos y tratados como consecuencia de los programas de vigilancia de las autoridades norteamericanas[27].

De hecho, algunos Estados miembros europeos, como Alemania, comenzaron a llevar a cabo acciones unilaterales frente a los Estados Unidos, en defensa de los datos de carácter personal de sus ciudadanos. Así, las autoridades alemanas de protección de datos, tanto federales como estatales, se pronunciaron de forma conjunta sobre el «acuerdo de puerto seguro», emitiendo un resolución, en julio de 2013, en la que se declaraba que, debido a las revelaciones sobre las actividades de vigilancia por los servicios de inteligencia y las agencias de seguridad norteamericana, no emitirían ninguna autorización más de transferencia internacional de datos a los Estados Unidos, mientras estudiaban la eventual suspensión de las transferencias internacionales de datos que ya se estaban llevando a cabo en virtud del «acuerdo de puerto seguro»[28]. Años después, el 19 de marzo de 2015 y de forma rotunda, la autoridad federal alemana de protección de datos (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) emitió un comunicado manifestando de manera explícita que el «acuerdo de puerto seguro» no proporciona un nivel adecuado de protección de los datos de carácter personal transferidos desde la Unión Europea a los Estados Unidos de Norteamérica[29].

Pese a todas estas denuncias, tanto las autoridades comunitarias como las empresas eran conscientes de que una suspensión del «acuerdo de puerto seguro» tendría consecuencias nefastas en las relaciones comerciales entre los Estados Unidos y la Unión Europea, por lo que la Comisión no se planteó suspender la decisión de adecuación que amparaba dicho acuerdo. Todo ello nos sitúa ante una cuestión mucho más amplia de la que ahora estamos analizando, esto es, ante los diferentes sistemas de protección de los datos de carácter personal que existen entre los Estados Unidos y la Unión Europea[30].

Sin embargo, como veremos a continuación, el «acuerdo de puerto seguro» sucumbió definitivamente cuando el TJUE dictó la sentencia, de 6 de octubre de 2015, en el asunto

---

27 Sobre el programa de vigilancia de la Agencia de Seguridad Nacional de los Estados Unidos, véase el Informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (A7- 0139/2014), de 21 de febrero de 2014. Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//ES

28 Dicha resolución está disponible (en inglés) en: http://www.bfdi.bund.de/SharedDocs/Publikationen/EntschliessungssammlungErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf?__blob=publicationFile

29 http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89DSK-SafeHarbor.html?cms_sortOrder=score+desc&cms_templateQueryString=safe+harbor

30 En relación con los diferentes estándares de protección de la privacidad en la Unión Europea en comparación con los Estado Unidos, véase, entre otros, el documento de la Administración Obama, de mayo de 2014, *Big Data: Seizing opportunities, preserving value y Big Data and privacy: a technological perspective*. También Álvarez Caro y Uriarte Landa (2014).

C-362/14, Maximilian Schreems vs. Data Protection Comisiones, donde declara inválida la Decisión 200/520/CE, de 26 de julio de 2000.

5. Análisis de la sentencia Schrems I (STJUE de 6 de octubre de 2015, en el asunto Maximilian Schreems vs. data protection comisiones de Irlanda)

Las duras críticas de la prensa estadounidense a la política de vigilancia e intromisión en la intimidad de los ciudadanos por parte de las autoridades norteamericanas[31], que pronto tuvo eco en toda la prensa mundial, así como los severos términos de la comunicación al Parlamento Europeo y al Consejo titulada «Restablecer la confianza en los flujos de datos entre la UE y EE. UU.», de 27 de noviembre de 2013, a la que acabamos de hacer referencia, provocó una creciente inquietud entre la población europea que facilitó el camino para que un ciudadano austriaco, el Sr. Schrems, se decidiera a iniciar un proceso judicial contra la empresa norteamericana Facebook, que culminó con la STJUE de 6 de octubre de 2015, mediante la que se declara inválida la Decisión de la Comisión 200/520/CE, de 26 de julio de 2000, o lo que es lo mismo, mediante la que se declara nulo el «acuerdo de puerto seguro».

El Sr. Schrems era usuario de la red social Facebook desde 2008, siendo importante aclarar, para entender el caso, que cualquier usuario de la Unión Europea que quiera utilizar esta red social debe firmar un contrato con Facebook Ireland, que es la filial europea de Facebook Inc. (esta última con domicilio social en los Estados Unidos), y que los datos de los usuarios europeos de Facebook Ireland son trasladados a los servidores centrales de Facebook Inc. situados en los Estados Unidos, donde son objeto de tratamiento.

Pues bien, esta sentencia resuelve la cuestión prejudicial planteada, con arreglo al artículo 267 del TFUE, por la High Court (Tribunal Superior de Irlanda) en el procedimiento entre Maximillian Schrems (usuario de la red Facebook) y el Data Protection Commissioner Ireland (Comisario para la Protección de Datos en Irlanda), denominado comúnmente como *commissioner* (comisario), que es la máxima autoridad irlandesa encargada de la protección de datos de carácter personal, quien se negó a instruir y tramitar la reclamación presentada

[31] Véanse los incisivos artículos publicados en *The Guardian* y *The Washington Post*, entre junio y agosto de 2013, entre otros: G. Greenwald: «NSA collecting phone records of millions of Verizon customers daily», en *The Guardian*, de 6 de junio de 2013; B. Gellman y L. Poitras: «U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program», en *The Washington Post*, de 7 de junio de 2013; G. Greenwald y E. Macaskill: «NSA Prism program taps in to user data of Apple, Google and others», en *The Guardian*, de 7 junio de 2013; N. Hopkins: «UK gathering intelligence via covert NSA operation», en *The Guardian*, de 7 de junio de 2013.

por el Sr. Schrems, basada en que Facebook Ireland transfería a Estados Unidos los datos personales de sus usuarios en Europa, almacenándolos en sus servidores estadounidenses, sin cumplir los principio exigidos en el «acuerdo de puerto seguro» previsto en la Decisión 2000/520/CE de la Comisión.

En su denuncia Schrems solicitaba que se prohibiera a Facebook Ireland la transferencia de los datos personales de sus usuarios al servidor de los Estados Unidos, alegando que la normativa jurídica de este país no garantizaba una protección suficiente de los datos personales de acuerdo con los estándares de la Unión Europea, lo que resultaba muy grave cuando la injerencia se producía como consecuencia de las actividades de vigilancia practicadas por las autoridades públicas norteamericanas, en clara referencia a las revelaciones de Edward Snowden sobre las actividades de los servicios de información de los Estados Unidos, en particular las de la Agencia de Seguridad Nacional de los Estados Unidos.

Sin embargo, y pese a la importancia de un tema que estaba siendo objeto de análisis por parte de los gobiernos de los Estados miembros de la Unión Europea, el comisario irlandés desestimó la reclamación al entender que no era competente para entrar a enjuiciar una materia que estaba amparada por la Decisión 2000/520/CE. En consecuencia, Schrems interpuso un recurso ante la High Court (Tribunal Supremo de Irlanda), órgano judicial que, tras examinar las pruebas presentadas por la parte denunciante, entendió que se encontraba ante un caso que sobrepasa el derecho irlandés, siendo de aplicación el derecho de la Unión Europea, pues existían serias dudas de que la Decisión 2000/520/CE se ajustara a las exigencias derivadas, tanto de los artículos 7 y 8 de la Carta, como de los principios enunciados por el Tribunal de Justicia en la sentencia Digital Rights Ireland y otros[32], pues el respeto a la vida privada garantizado en el artículo 7 de la Carta quedaría privado de efectividad si se permitiera a los poderes públicos norteamericanos acceder a las comunicaciones electrónicas y a los datos de carácter personal de manera aleatoria y generalizada, sin ninguna justificación objetiva y motivada, fundada en motivos de seguridad nacional, que, en todo caso, deberían estar regulados de forma clara y previsible y con supervisión judicial. En consecuencia, elevó al TJUE sendas cuestiones prejudiciales.

La primera de las cuestiones prejudiciales planteadas permitió al Tribunal de Justicia dictar jurisprudencia dirigida a la delimitación del ámbito de competencias de las autoridades de control de cada uno de los Estados miembros (el Data Protection Commissioner en Irlanda, o la Agencia Nacional de Protección de datos en el caso español), así como la ex-

[32] C293/12 y C594/12, EU: C:2014:238. Se trata de la Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014, en la que resuelve sendas peticiones de decisión prejudicial planteadas, con arreglo al artículo 267 TFUE, por la High Court (Irlanda) y el Verfassungsgerichtshof (Austria), y en la que el TJUE declara inválida la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

tensión territorial de sus facultades de control cuando, como es el caso, el tratamiento de los datos personales no solo tiene lugar fuera de las fronteras del Estado en el que dicho órgano de control ejerce su labor, sino fuera de la Unión Europea. Según entiende el TJUE, las autoridades nacionales de control están encargadas del correcto cumplimiento de las reglas de la Unión para la protección de las personas físicas frente al tratamiento de datos personales, concluyendo que «toda autoridad nacional de control está investida, por tanto, de 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 95/46» (apartado 47), concluyendo que la Decisión 2000/520/CE no puede en ningún caso impedir «que las personas cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país, presenten a las autoridades nacionales de control una solicitud, prevista en el art. 28.4 de la Directiva 95/46, para la protección de sus derechos y libertades» (apartado 53), sin perjuicio de que, en caso de que se considere fundada la denuncia, se tenga que trasladar el caso al Tribunal de Justicia competente, para que eleve una cuestión prejudicial al TJUE.

Una vez aclarada la extensión de las facultades de las autoridades de control de protección de datos de los Estados miembros, el TJUE pasa a examinar la segunda de las cuestiones prejudiciales planteadas, relativa a si el ordenamiento jurídico de los Estados Unidos de América garantiza un nivel de protección adecuado de los datos personales trasferidos desde la Unión Europea y, en consecuencia, si la Decisión 2000/520/CE y los «principios de puerto seguro» que figuran su anexo I se ajustan a las exigencias derivadas de la Directiva 95/46/CE, interpretada a la luz de la Carta.

El Tribunal constata que, en virtud del anexo I de la Decisión 2000/520/CE, los «principios de puerto seguro» son aplicables únicamente a las entidades y empresas estadounidenses «autocertificadas» que reciban datos personales desde la Unión como consecuencia del comercio internacional, pero no se extienden a las autoridades del país, que también pueden acceder a dichos datos como dispone el anexo I, por «exigencias de seguridad nacional, interés público y cumplimiento de la ley». En consecuencia, aunque el TJUE no lo dice de forma explícita, da a entender que la Decisión 2000/520/CE abre la puerta para que las autoridades norteamericanas accedan de manera indiscriminada y sin ningún tipo de control a los datos de carácter personal que llegan desde la Unión Europea a empresas de los Estados Unidos, dado el carácter general de la excepción prevista en el anexo I.

En esta sentencia el TJUE fija una doctrina que resulta muy relevante en relación con los estándares de protección de los datos de carácter personal que debe garantizar la Unión y que se extienden a las transferencias de datos personales a países terceros. Doctrina que puede sintetizarse en los siguientes puntos:

a) Toda normativa que autorice un límite en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta debe contener «reglas claras y precisas

que regulen el alcance y la aplicación» de la injerencia (apartado 91); asimismo deberá contener los criterios objetivos que permitan determinar los casos en los que cabe que una autoridad pública pueda acceder y utilizar los datos personales (apartado 94).

b) Supone una clara lesión del derecho fundamental a la tutela judicial efectiva reconocido en el artículo 47 de la Carta la imposibilidad de que el justiciable ejerza acciones para acceder a sus datos personales o para conseguir su rectificación o supresión (apartado 95).

c) Se requiere una constatación debidamente motivada de que el tercer país «garantiza efectivamente un nivel de protección de los derechos fundamentales sustancialmente equivalente al garantizado en el ordenamiento jurídico de la Unión» (apartado 96).

d) Las autoridades nacionales de control tienen la facultad de examinar cualquier solicitud frente a todo tratamiento de datos personales, aunque ello implique poner en cuestión la validez de una decisión de la Comisión (apartado 99, en conexión con los apartados 53, 57 y 63).

De acuerdo con esta doctrina, el TJUE declara inválida la Decisión 2000/520/CE, al entender que la Comisión no constató suficientemente la existencia de un nivel de protección adecuado de los datos de carácter personal transferidos a los Estados Unidos, unido al hecho de que el artículo 3.1 de la Decisión 2000/520/CE priva a las autoridades nacionales de control de las facultades que les atribuye el artículo 28 de la Directiva 95/46/CE.

6. Consecuencias de la sentencia Shrems I: de la nulidad del «acuerdo de puerto seguro» (*safe harbour*) a la aprobación del «acuerdo de escudo de privacidad» (*privacy shield*)

Tras la sentencia Schrems I, que declaró inválida la Decisión 2000/520/CE de la Comisión, todas las entidades estadounidenses antes adheridas al «acuerdo de puerto seguro»[33] perdieron su condición de «entidad con un nivel de protección adecuado» para la recepción de datos personales desde un Estado miembro de la Unión Europea.

Ante la falta de una decisión de adecuación de la Comisión, la única puerta para realizar transferencias de datos entre la Unión Europea y los Estados Unidos de América se encontraba en el artículo 26.1 de la Directiva 95/46/CE, que regulaba la posibilidad de que

[33] Según el punto 2.2 de la Comunicación COM (2013) 847 final, a 26 de septiembre de 2013 estaban certificadas un total de 3.246 entidades.

los Estados miembros pudieran efectuar transferencias de datos a un país tercero que no garantizase un nivel adecuado de protección, siempre que el interesado otorgara su consentimiento o la transferencia de datos fuera imprescindible para la ejecución de un contrato, entre otros supuestos. Con este catálogo de posibilidades se buscaba no bloquear, ni entorpecer, las relaciones económicas y comerciales entre Europa y terceros países, pero dejaban al afectado ante una situación de total indefensión, pues en la mayoría de los casos debía optar entre proteger sus datos personales o sus intereses comerciales, esto es, se le colocaba ante la tesitura de tener que renunciar a un derecho fundamental para que su negocio o sus legítimos intereses económicos o sociales salieran adelante, lo que no parece muy conciliable con la posición que tienen los derechos fundamentales en el Estado de derecho.

Es cierto que la regulación de la protección de datos en la Unión Europea reconoce el consentimiento como un elemento esencial del derecho a la protección de los datos personales, como se desprende del artículo 8 de la CDFUE, que recoge que los datos personales «se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley», y que, por tanto, se configura como una facultad que permite a los titulares del derecho actuar con autonomía, pudiendo controlar el acceso y tratamiento de los mismos. Sin embargo, creo que la exigencia derivada del artículo 25.1 de la Directiva 95/46/CE, según la cual las transferencias de datos personales a países terceros solo podían realizarse cuando dicho país garantizase «un nivel de protección adecuado», quedaría vacía de contenido si cede con el solo consentimiento del interesado, tal y como parece desprenderse del artículo 26.1 a) de la Directiva 95/46/CE.

A las excepciones del artículo 26.1 debemos añadir lo previsto en el segundo apartado de este precepto, que recogía, sin perjuicio de lo previsto en el apartado anterior, que los Estados miembros podían autorizar una transferencia de datos personales a un tercer país que no garantice un nivel de protección adecuado «cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas» (art. 26.2).

Pues bien, los instrumentos utilizados para garantizar este «nivel de protección adecuado» de los datos de carácter personal ante la ausencia de una decisión de adecuación de la Comisión serán, por un lado, las «cláusulas contractuales tipo» (en aquellos casos en los que las transferencias se realizan en el marco de un contrato) y, por otro, las «normas corporativas vinculantes» (cuando la transferencia se realice entre entidades de un mismo grupo empresarial).

Así, las «cláusulas contractuales tipo» se configuran como un instrumento que permite a los responsables del tratamiento realizar transferencias internacionales de datos personales

con ciertas garantías, subscribiendo un contrato entre el importador y el exportador de los datos. Mediante estas cláusulas se deben determinar aquellas medidas de seguridad que han de ser aplicadas por la entidad o empresa encargada del tratamiento de datos del tercer país que no ofrece la protección adecuada según la Comisión. El importador de datos únicamente podrá tratar los datos personales transferidos de conformidad con las instrucciones recibidas y las obligaciones impuestas en las cláusulas[34].

Por otro lado, las «normas corporativas vinculantes» se refieren a códigos de conducta vinculantes dentro de un conjunto de empresas pertenecientes al mismo grupo, cuya finalidad es la de ofrecer garantías suficientes cuando los datos personales van a ser transferidos a una filial, o empresa del mismo grupo, situado en un país que no cuenta con un nivel de protección adecuado.

El medio para la aprobación de unas y otras es diferente: las «cláusulas contractuales tipo» deberán ser adoptadas por la Comisión por medio de decisiones, de acuerdo con lo previsto en el artículo 26.4 de la Directiva 95/46/CE, mientras que las «normas corporativas vinculantes» deberán ser aprobadas por las autoridades de control de protección de datos de los diferentes Estados miembros, valorando su adecuación a los principios de la Directiva 95/46/CE.

En todo caso, lo cierto es que la nulidad del «acuerdo de puerto seguro», como consecuencia de la sentencia Schrems I, dejó una situación de cierto vacío normativo y, por tanto, de inseguridad, al no existir un instrumento jurídico general para asegurar la protección de datos en las relaciones comerciales entre Europa y los Estados Unidos, sin que resultara asumible que las relaciones comerciales se vieran afectadas negativamente, por lo que comenzaron las conversaciones entre el Consejo y las autoridades estadounidenses para alcanzar una nueva decisión de adecuación que permitiera un cómodo tráfico de datos personales con los Estados Unidos, negociaciones que tuvieron como resultado la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, sobre la adecuación de la protección conferida por el «escudo de la privacidad UE-EE. UU.», que sustituye el anulado «acuerdo de puerto seguro», por el ahora denominado «acuerdo de escudo de privacidad» (*privacy shield*), que imponía obligaciones más estrictas a las empresas estadounidenses en la protección de los derechos de privacidad de los ciudadanos de la Unión Europea, pero que, sobre todo, fijaba un nuevo marco jurídico que pretendía ser más restrictivo con la intervención de la Agencia de Seguridad Nacional norteamericana en el acceso a los datos personales de ciudadanos de la Unión Europea, exigiendo que el ordenamiento de los Estados Unidos ofrezca a los ciudadanos europeos afectados recursos administrativos y judiciales ante las autoridades estadounidenses.

[34] Véase la Decisión de la Comisión 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/CE del Parlamento Europeo y del Consejo.

En esta decisión la Comisión indica, en síntesis[35], que se ha producido una mejora en las garantías de protección de los datos personales trasferidos desde la Unión Europea a los Estados Unidos, pues el Gobierno estadounidense, a través de la Oficina del Director de Inteligencia Nacional, ha proporcionado a la Comisión una relación de compromisos concretos y detallados (que se recogen en el anexo VI de la decisión de ejecución), a lo que se une una carta firmada por el secretario de Estado (que también se incluye en la decisión, como anexo III), mediante la que el Gobierno de los Estados Unidos se compromete a crear un nuevo mecanismo de supervisión de las injerencias en los datos de carácter personal con fines de seguridad nacional, que recaerá en una figura creada *ad hoc*, el «defensor del pueblo en el ámbito del escudo de la privacidad», que será independiente de los servicios de inteligencia.

La Comisión también indica que la declaración del Departamento de Justicia de los Estados Unidos (contenida en el anexo VII de la decisión) describe un conjunto de garantías que han de cumplir los poderes públicos que accedan a datos de carácter personal de ciudadanos comunitarios, y, por último, con la finalidad de asegurar la transparencia y reflejar la naturaleza jurídica de estos compromisos, cada uno de los documentos anteriormente citados y adjuntos a la decisión deberán publicarse en el Registro Federal de los Estados Unidos.

De lo expuesto se desprende que la sentencia Schrems I empujó a la Unión Europea a exigir a los Estados Unidos de Norteamérica mayores garantías en la protección de datos de carácter personal pues, caso contrario, las relaciones comerciales podrían verse afectadas seriamente. Sin embargo, como veremos a continuación, esta aparente resolución del conflicto duró poco tiempo, pues la STJUE Schrems II, de 16 de julio de 2020, declaró inválida la Decisión de Ejecución 2016/1250 de la Comisión, de 12 de julio de 2016, poniendo de relieve, de nuevo, que los Estados Unidos de América no son un destino seguro para los datos personales de los ciudadanos de la Unión Europea.

7. La sentencia Schrems II (STJUE de 16 de julio de 2020, en el asunto *data protection* comisiones y Schrems vs. Facebook Ireland)

Como consecuencia del fallo de la sentencia Schrems I, la High Court de Irlanda devolvió la reclamación del Sr. Schrems al Comisario, para que continuara con el procedimiento y realizara las investigaciones pertinentes. En este sentido, el comisario llegó a la conclusión de que sin la cobertura jurídica de una decisión de adecuación de la Comisión, los

[35] Síntesis realizada a partir del considerando número 65 de la decisión que estamos analizando.

datos personales que se transferían desde Europa a Facebook Inc. únicamente contaban con la protección de «cláusulas contractuales tipo», en los términos regulados en la Decisión de la Comisión 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/CE del Parlamento Europeo y del Consejo (hay que tener en cuenta que en esta fecha aún no se había aprobado la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, sobre la adecuación de la protección conferida por el escudo de la privacidad UE-EE. UU., que, como hemos comentado anteriormente, sustituye el «acuerdo de puerto seguro» por el «acuerdo de escudo de privacidad»). Ante esta situación el comisario sugirió al Sr. Schrems que modificara su reclamación.

El 1 de diciembre de 2015 el Sr. Schrems planteó una nueva reclamación en la que alegaba que el gobierno estadounidense obligaba a Facebook Inc. a poner a disposición de autoridades como la NSA y el FBI (Federal Bureau of Investigation) los datos transferidos a dicha empresa desde la Unión Europea, llevándose a cabo programas de vigilancia incompatibles con los artículos 7, 8 y 47 de la CDFUE y, por ello, solicitó al comisario la suspensión de las transferencias de sus datos personales a Facebook Inc.

El 24 de mayo de 2016 el comisario publicó las conclusiones provisionales de su investigación, en las que se reflejaba que, tal y como denunciaba el Sr. Schrems, los datos personales de los ciudadanos de la Unión trasferidos a los Estados Unidos corrían el riesgo de ser consultados y tratados de manera masiva e indiscriminada por las autoridades de los Estados Unidos, lo que, a su juicio, no resultaba subsanado por las «cláusulas contractuales tipo» previstas en Decisión de la Comisión de 5 de febrero, anteriormente mencionada, pues dichas cláusulas solo conferían a los interesados derechos contractuales contra el exportador o el importador de los datos, pero no vinculaban a las autoridades estadounidenses.

Por ello, el Comisario elevó, el 31 de mayo de 2016, un recurso ante la High Court apoyándose en la jurisprudencia resultante de la STJUE Schrems I. La High Court admitió a trámite el recurso y, una vez iniciado el procedimiento, decidió, con fecha 4 de mayo de 2018, elevar una cuestión prejudicial al TJUE, al entender que la reclamación afectaba a la validez de la Decisión 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».

Es de señalar que en el recurso elevado por el comisario a la High Court se cuestiona únicamente la validez de la referida Decisión de la Comisión de 5 de febrero, pues ya hemos indicado que fue presentado ante el órgano jurisdiccional antes de que se aprobara la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, que recoge el «acuerdo de escudo de privacidad», que, al menos teóricamente, imponía obligaciones más estrictas a las empresas estadounidenses en la protección de los datos personales que son

transferidos desde la Unión Europea y exigía una intervención más restrictiva y controlada por parte de la Agencia de Seguridad Nacional norteamericana.

Ahora bien, la High Court sí hace referencia a la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, cuando pregunta al TJUE acerca de la protección que debe otorgarse a las transferencias internacionales de datos en virtud de los artículos 7, 8 y 47 de la Carta, razón por la que el Tribunal de Justicia considera que debe tomarse en consideración esta última decisión de ejecución de la Comisión, vigente desde el 12 de julio de 2016. Asimismo, es importante señalar que en el momento en el que el TJUE resuelve esta nueva cuestión, el canon de adecuación a la Carta de Derechos Humanos ya se hace desde el contenido del RGPD. En este sentido ha de tenerse en cuenta que el artículo 45.2 a) del RGPD recoge, como requisitos necesarios para la transmisión de datos personales a un país no miembro de la Unión Europea, la existencia de «garantías adecuadas», tales como «el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional», a lo que se añade, en ese mismo apartado, la necesidad de que los interesados cuenten con «recursos administrativos y acciones judiciales que sean efectivos». Lo que de manera más sintética recoge el artículo 44 del RGPD, según el cual el tercer país deberá garantizar un nivel de protección equivalente al asegurado dentro de la Unión Europea.

Estas exigencias no son meramente orientativas, pues en aquellos casos en los que el tercer país no asegure tal protección, por medio de su legislación interna o sus compromisos internacionales, deberá prohibirse la transferencia de datos personales desde la Unión Europea.

Asimismo, el Tribunal Europeo de Derechos Humanos reitera que la autoridad de control competente de cada Estado miembro tiene la obligación de prohibir o suspender una transferencia de datos personales a un país tercero en aquellos casos en los que considere que las «cláusulas contractuales tipo» de protección de datos adoptadas por la Comisión no son respetadas, o lo que es más importante, no pueden ser respetadas, pues la normativa o la práctica de las autoridades de dicho país no aseguran un nivel de protección similar al existente en la Unión Europea.

Pues bien, para facilitar el cumplimiento de su misión y la posibilidad de tramitar las reclamaciones presentadas, el artículo 58.1 del RGPD atribuye a las autoridades de control importantes poderes de investigación, por lo que el TJUE indica que cuando una de esas autoridades entiende, al finalizar su investigación, que el interesado cuyos datos personales se transfirieron a un país tercero no goza en ese país de un nivel de protección adecuado,

está obligada, en aplicación del derecho de la Unión, a reaccionar con el fin de subsanar la insuficiencia constatada.

El TJUE entiende que la Decisión de la Comisión de 5 de febrero de 2010 es válida, teniendo en cuenta que, según se dispone en su texto, el responsable del tratamiento de datos de la Unión y el destinatario de la transferencia de datos personales que se encuentra en el tercer país están obligados a comprobar, antes de que tenga lugar la transferencia internacional de datos, que en el país tercero existe una legislación que va a respetar la «cláusula contractual tipo» en cuestión, lo que incluye a las autoridades públicas. Asimismo, el destinatario de esa transferencia tiene, según la referida decisión, la obligación de informar al responsable del tratamiento de datos europeo de su eventual incapacidad para cumplir con esas cláusulas en caso de que la autoridad pública le exija la cesión de los datos personales que se encuentran en sus bases de datos, o en caso de que se produzca un cambio legislativo que pueda causar un efecto negativo sobre las garantías de protección de los datos personales transferidos. Garantías que el TJUE considera suficientes.

Por lo tanto, el TJUE concluye que la decisión cuya validez se cuestiona prevé mecanismos efectivos que garantizan una correcta protección de los datos personales transferidos a un tercer país, por lo que no se puede considerar que los artículos 7, 8 o 47 de la Carta resulten vulnerados (apartado 149).

El TJUE insiste en que, si bien la demanda elevada por el comisario cuestiona únicamente la validez de la Decisión de la Comisión de 5 de febrero de 2010, relativa a las «cláusulas contractuales tipo», pues dicho recurso fue presentado antes de que se adoptara la Decisión de Ejecución de la Comisión de 12 de julio de 2016, sobre la adecuación de la protección conferida por el escudo de privacidad entre la Unión Europea y los Estados Unidos, lo cierto es que para resolver las cuestiones prejudiciales planteadas resulta necesario tener en cuenta también esta última decisión de ejecución; estudiando así la protección exigida por el RGPD queda suficientemente garantizada con la posterior Decisión de Ejecución de la Comisión de 12 de julio de 2016, que fija el «acuerdo de escudo de la privacidad».

Se cuestiona la adecuación declarada por la Comisión en la Decisión de Ejecución de 12 de julio de 2016, porque, según examina el TJUE, las injerencias resultantes de los programas de vigilancia basados en el artículo 702 de la FISA (Foreign Intelligence Surveillance Act) y en la Executive Order 12333 no están sujetas a exigencias que garanticen, dentro del respeto del principio de proporcionalidad, un nivel de protección sustancial equivalente al garantizado por el artículo 52, apartado 1, segunda frase, de la Carta. Por tanto, es preciso examinar si esos programas de vigilancia se aplican respetando tales exigencias (apartado 178).

Así, y en lo que se refiere a los programas de vigilancia basados en el artículo 702 de la FISA, la Comisión constató, en el considerando 109 de la Decisión de Ejecución de 12 de julio de 2016, que el FISC (United States Foreign Intelligence Surveillance Court) no autoriza

medidas de vigilancia individuales, sino programas de vigilancia muy generales (como PRISM o Upstream), por lo que el TJUE concluye que mediante estos sistemas se obtiene mucha información de manera indiscriminada, pero sin seleccionar previamente a las personas investigadas y, por tanto, sin conocer con precisión y de forma individualizada si constituyen algún tipo de amenaza para la seguridad nacional (apartados 179 y ss.).

En consecuencia, el TJUE afirma que «resulta evidente que del artículo 702 de la FISA en modo alguno se desprende la existencia de limitaciones a la habilitación que dicho artículo otorga para la ejecución de programas de vigilancia con fines de inteligencia exterior ni tampoco la existencia de garantías para las personas no nacionales de los Estados Unidos que sean potencialmente objeto de esos programas» (apartado 180). A estos argumentos se une la constatación de que la figura del Defensor del Pueblo, creada por los Estados Unidos en el ámbito del «escudo de privacidad», no es suficiente para subsanar estas deficiencias. En primer lugar, porque se pone en entredicho la independencia de esta figura, que es nombrado y destituido por el secretario de Estado (apartado 195) y porque, en todo caso, no resulta suficiente para subsanar la ausencia de garantías jurisdiccionales efectivas contra la intervención de los programas de vigilancia basados en el artículo 702 de la FISA y en la Executive Order 12333 (apartado 192).

En atención a todo lo expuesto, el TJUE concluye que la Decisión de Ejecución de la Comisión de 12 de julio de 2016, sobre la adecuación de la protección conferida por el escudo de privacidad entre la Unión Europea y los Estados Unidos es inválida, al ser incompatible con el artículo 45.1 del RGPD, interpretado a la luz de los artículos 7, 8 y 47 de la Carta.

8. Consecuencias de la sentencia Schrems II: la nulidad del «acuerdo de escudo de privacidad» y la pérdida de fiabilidad de las decisiones de adecuación de la Comisión Europea

Tras la STJUE Schrems II, el «escudo de privacidad» entre la Unión Europea y los Estados Unidos dejó de ser un mecanismo adecuado para garantizar el cumplimiento de los requisitos exigidos por la Unión Europea en materia de protección de datos, por lo que, al igual que ocurrió tras publicarse la STJUE Schrems I, las transferencias internacionales de datos entre la Unión Europea y los Estados Unidos quedaron sumidas en un limbo jurídico, con la consiguiente incertidumbre de las empresas, expuestas a ser sancionadas por la Unión Europea con cuantiosas multas si no suspendían el flujo de datos personales o estableciían algún tipo de garantía alternativa.

Resultaba evidente que la nulidad de la Decisión de Ejecución de la Comisión de 2016, relativa a la adecuación de la protección conferida por el «escudo de privacidad», iba a tener

un impacto negativo en las relaciones entre los Estados Unidos y la Unión Europea, tanto políticas como comerciales, e iba a suponer un serio obstáculo para todas aquellas empresas que necesitan realizar transferencias internacionales de datos personales para efectuar sus actividades económicas, lo que afecta, sobre todo, a aquellas que ofrecen «servicios digitales», cuyo aumento exponencial hace que ya se hable de «la economía digital» como la única vía de las relaciones comerciales en un futuro muy cercano[36], lo que ya es una realidad respecto de las actividades que se materializan a través de servicios de *cloud computing*[37].

Por todo ello, el TJUE se planteó la opción de mantener los efectos de la decisión de ejecución de la Comisión declarada inválida, para evitar una situación de vacío legal (apartado 202), encontrando finalmente una salida en el artículo 49 del RGPD, del que se desprende la posibilidad de que puedan realizarse transferencias de datos personales a países terceros en ausencia de una decisión de adecuación de la Comisión, siempre que (en síntesis): a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos que asume, debido a la ausencia de una decisión de adecuación; b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento, o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado, o para la celebración o ejecución de un contrato entre el responsable del tratamiento y otra persona física o jurídica; c) la transferencia sea necesaria por razones importantes de interés público; d) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones, o para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; e) la transferencia se realice desde un registro público que, con arreglo al derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero solo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el derecho de la Unión o de los Estados miembros para la consulta.

Como se puede apreciar, estamos ante un precepto muy similar al antiguo artículo 26 de la Directiva 95/46/CE, en el que el consentimiento del interesado en la cesión y en el tratamiento de sus datos de carácter personal a un tercer país se convierte en la vía fácil para superar todas las exigencias derivadas de las normas jurídicas de la Unión Europea en ma-

---

[36] Resulta interesante, por lo que tuvo de pionero, Tapscott (1997). El término «economía digital» se generalizó tras la publicación del citado libro de Tapscott, en el que se auguraba, en la década de los noventa, cómo internet iba a cambiar la forma de hacer negocios. De hecho, se trata de una de las obras más vendidas en 1997, apareciendo en diversas listas de *best-sellers*, así como en la lista de libros de negocios del *New York Times* y en la lista de *BusinessWeek*.

[37] El *cloud computing*, conocido también como «servicios en la nube» o «informática en la nube», es un paradigma que permite ofrecer servicios digitales de muy distinta naturaleza a través de una red, que usualmente es internet. Un estudio de los comienzos de esta figura en Torres Viñals (2012). Desde un enfoque jurídico, Martínez Martínez (2012).

teria de protección de datos de carácter personal, pues si el interesado desea obtener determinados servicios de una empresa norteamericana, o mantener relaciones comerciales, ha de consentir la cesión de sus datos a dicha empresa y asumir la posible intervención de las autoridades norteamericanas.

En cuanto al consentimiento, parece claro que debe prestarse de forma explícita para cada cesión concreta de datos personales, siendo necesario que la empresa o entidad receptora informe previamente al interesado de los riesgos que puede implicar una transferencia de datos personales que no esté amparada por una decisión de adecuación de la Comisión. De hecho, en el caso Schrems II, el TJUE constató que la cesión de datos personales a Facebook Inc. no podía ampararse en el consentimiento explícito de los afectados, pues dicha transferencia se realizó sobre la base de cláusulas tipo, que no incorporan un consentimiento indubitado y específico para cada uno de los datos transferidos (Miguel Asensio, 2020, p. 7).

Pues bien, una vez anulada la decisión de adecuación, el Comité Europeo de Protección de Datos (*European Data Protection Board*) publicó un documento, con fecha de 24 de julio de 2020, en el que, bajo el título *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18. Data Protection Commissioner v Facebook Ireland Ltd. and Maximillian Schrems*, analiza algunas de las consecuencias de la sentencia.

En este sentido, el Comité Europeo de Protección de Datos entiende que de la sentencia se desprende que no existe un periodo de gracia durante el cual se pueda mantener la transferencia de datos a los Estados Unidos, pues tras demostrarse que dicho país no ofrece un nivel de protección equivalente al de la Unión Europea, todas las transferencias de datos pasan, con carácter general, a considerarse ilegales[38]. En el documento también se indica que cabe la posibilidad de mantener las transferencias de datos personales si existen «condiciones generales de contratación» y «normas corporativas vinculantes», debiendo tenerse en cuentas las circunstancias concretas de las transferencias y la evaluación realizada por las autoridades del control, pudiendo ser igualmente necesaria la inclusión de medidas suplementarias para garantizar la protección de los datos personales[39].

Por último, el Comité Europeo de Protección de Datos insiste en que el consentimiento del interesado pasa a convertirse en la única vía para la mayoría de las transferencias internacionales de datos hacia terceros países que no cuentan con una decisión de adecuación, siempre que sea explícito, específico sobre los datos personales a transferir e informado, pues el interesado ha de conocer todos riesgos que asume como consecuencia de la inexistencia de garantías suficientes en el país de recepción de sus datos personales.

[38] Lo que se desprende de la respuesta a la pregunta 4 del documento, al que se puede acceder en el enlace: https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

[39] Tal y como se deduce de la respuesta a las preguntas 5 y 6.

En consecuencia, la transferencia de datos de carácter persona entre la Unión Europea y los Estados Unidos vuelve a la situación en la que se encontraba en octubre de 2015, tras la STJUE Schrems I, esto es, se retorna a un escenario que se caracteriza por la ausencia de un marco jurídico general que asegure una protección efectiva de los datos personales de los ciudadanos europeos que llegan a los Estados Unidos, por lo que las empresas se ven en la necesidad de buscar soluciones *ad hoc* para no suspender sus relaciones comerciales, intentando encontrar una salida jurídica, no solo acudiendo a los supuesto previstos en el artículo 49 del RGPD, anteriormente reproducido, sino también mediante la utilización de alguno de los mecanismos subsidiarios de protección regulados en los artículos 45 y siguientes del RGPD, que analizaremos con detalle más adelante, de entre los que destaca la utilización de «condiciones generales de contratación» aceptadas por el interesado.

Así, empresas como Twitter, YouTube o Facebook, entre otras muchas, han elaborado políticas de cesión y tratamiento de datos que los usuarios de estas redes sociales han de asumir si quieren participar de sus servicios[40], por lo que, una vez más, parece que la cláusula de cierre de la normativa europea en materia de protección de datos de carácter personal es, simple y llanamente, que el interesado renuncie a tal protección.

Por otro lado, la declaración de nulidad de la decisión de adecuación de la Comisión relativa al *privacy shield* tiene lugar cinco años después de la anulación de la decisión de la Comisión relativa al *safe harbour*, lo que conduce a cuestionar la eficacia de las decisiones de adecuación de la Comisión.

Como se puede deducir de lo expuesto en las páginas precedentes, gran parte de las razones que llevaron a la nulidad del *privacy shield* por la STJUE Schrems II habían sido anteriormente criticadas por la STJUE Schrems I, lo que lleva a sospechar que los cambios introducidos en el segundo de los acuerdos y las conversaciones mantenidas entre los Estados Unidos y Europa han sido papel mojado y la Comisión no ha resultado un órgano eficaz en la protección de los derechos fundamentales de los ciudadanos comunitarios. No se prevé una tercera decisión de adecuación, como apunta parte de la doctrina, pues ello supondría la pérdida total de credibilidad de la Comisión en el desarrollo de su función de protección de los derechos de los ciudadanos europeos en las negociaciones internacionales (Costello, 2020, p. 16), pues no se espera que los Estados Unidos modifiquen sus políticas de vigilancia[41], dada la permanencia de instrumentos de vigilancia como los recogidos en la FISA o en la Executive Order 12333, en concreto los programas PRISM y Upstream (Butler, 2017, p. 112).

---

40 Un interesante análisis de los códigos privados de conducta de las empresas que operan en redes sociales en García-Perrote Martínez y Gabriel García-Micó (2020, pp. 555 y ss.).

41 Sobre el acceso a los datos de carácter personal por pate de las autoridades norteamericanas, Chander (2020, p. 775).

Por tanto, anulados sendos acuerdos, la facultad de determinar y evaluar las garantías necesarias para reanudar las transferencias de datos a los Estados Unidos se traslada a las autoridades de control de los países miembros y, en última instancia, a los encargados del tratamiento de datos de las empresas implicadas, lo que les obliga a estos últimos (entidades privadas) a conocer en profundidad la legislación nacional y comunitaria, trasladándoles importantes responsabilidades y dando lugar a opiniones dispares entre unas empresas y otras[42].

Los estudios jurídicos que han abordado esta materia tras la sentencia Schrems II exponen la situación de hecho que tiene lugar tras la nulidad del acuerdo de *privacy shield* y denuncian la falta de alternativas jurídicas generales para solventar esta situación, al entender, por un lado, que las «cláusulas tipo» de protección de datos no son una opción, pues una transmisión de datos personales a un tercer país solo podrá llevarse a cabo bajo la exclusiva protección de dichas cláusulas cuando en ese país se asegure un nivel de protección equivalente al que se garantiza en la Unión Europea (Tracol, 2020, p. 5; Maldonado, 2020, p. 10) y, por otro, que tampoco resultan eficaces «las normas corporativas vinculantes», pues su existencia «no implica que haya una protección suficiente en un tercer país, sino que esto se tendrá que comprobar en cada caso y añadir garantías adicionales cuando fuese necesario» (Fuentes Máiquez, 2021, p. 8).

9. Conclusiones

Tras las declaraciones de nulidad de las decisiones de adecuación de la Comisión respecto de los Estados Unidos, como consecuencia de las STJUE Schrems I y Schrems II, no solo se puso en entredicho el papel de la Comisión como órgano que aseguraba la protección de los datos personales en las transferencias internacionales de datos, sino que también se empezó a cuestionar la eficacia práctica de las normas jurídicas de la Unión, pues, en la medida en que los distintos niveles de garantías jurídicas que se regulan en el RGPD van fallando, ya sea por la intervención de las autoridades de un tercer país invocando «razones de seguridad nacional», como es el caso de los Estados Unidos, ya sea por el eventual uso desleal de estos datos por las empresas receptoras, la única salida que tiene el afectado es prestar su consentimiento para la cesión y tratamiento de sus datos personales, aceptando las posibles consecuencias negativas, relativas a un uso incorrecto de los mismos. Llegados a este punto, el interesado tiene que optar entre mantener relaciones comerciales con entidades públicas o privadas de determinados Estados o preservar sus datos personales frente a un uso indebido de los mismos.

[42] Lo que pone de relieve Fuentes Máiquez, (2021, p. 10), coincidiendo en este punto con lo que, años antes de que se dictara la STJUE Schrems II, ya auguraba parte de la doctrina, como Bennett (2016).

No obstante, los distintos órganos de la Unión Europea siguen emitiendo documentos jurídicos, con mayor o menor valor vinculante, en su intento por mantener un nivel de protección adecuado de los datos personales de los ciudadanos comunitarios. Así, el 10 de noviembre de 2020, el Comité Europeo de Protección de Datos adoptó las recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para asegurar el cumplimiento del nivel de protección de datos personales de la Unión Europea, a través de las que desarrolla una guía explicativa para orientar a los exportadores e importadores de datos personales sobre las garantías que han de ser aplicadas durante las transferencias de los datos.

De estas recomendaciones se desprende que el Comité Europeo de Protección de Datos reconoce el importante papel que se otorga a los responsables de las transferencias de datos personales de las empresas, quienes tienen la obligación de verificar, de manera individualizada, si la legislación o práctica del tercer país puede afectar a la eficacia de las garantías contenidas en la legislación europea. En aquellos casos en los que estos responsables se percaten de la existencia de algún tipo de laguna o deficiencia en la protección ofrecida por el país receptor de los datos personales, los responsables de la transferencia deberán aplicar aquellas medidas complementarias que consideren necesarias para paliar las mencionadas carencias.

En conclusión, la búsqueda de mecanismos jurídicos dirigidos a garantizar el derecho fundamental a la protección de datos de carácter personal en el ámbito de las transferencias internacionales de datos entre un Estado europeo y un tercer Estado ha sido uno de los objetivos de la Unión Europea, primero a través de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, 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 y, posteriormente, en el Reglamento general de protección de datos del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Mediante estas normas la Unión Europea no se ha limitado a asegurar un nivel uniforme de protección de este derecho en las legislaciones de los Estados miembros, sino que también exige que desde Europa solo se envíen datos personales a terceros países que garanticen un estándar de protección similar al existente en la Unión Europea, prohibiendo o suspendiendo aquellas relaciones comerciales que impliquen un flujo de datos personales hacia Estados en los que no se cuenta con «un nivel de protección adecuado», lo que supone una medida eficaz para la defensa del derecho fundamental a la protección de datos de carácter personal, pero que tiene un efecto negativo en las relaciones comerciales, razón por la que ha sido necesario fijar un conjunto de excepciones a esta regla general de protección, tal y como se analiza con detenimiento en el texto.

Las «decisiones de adecuación» de la Unión Europea no ha resultado eficaces, optando por la utilización de las «cláusulas contractuales tipo» (que han de ser aprobadas por la Comisión y operan cuando las transferencias se realizan en el marco de un contrato) y por las «normas corporativas vinculantes» (cuando la transferencia de datos se realice entre

entidades de un mismo grupo empresarial). Ahora bien, en el caso de que no sea posible la utilización de ninguno de los instrumentos anteriores y el país receptor de los datos personales no garantice un nivel de protección similar al que rige en la Unión Europea, la normativa prevé una serie de excepciones, de tal manera que la transferencia internacional de datos podrá efectuarse si se cuenta con el consentimiento inequívoco del interesado, requisito que ha de unirse a la necesidad de celebrar o ejecutar un contrato en interés del particular o que afecta a los intereses comerciales generales.

Tras las STJUE Schrems I y Schrems II, que anulan sendas decisiones de adecuación de la Comisión, queda claro que los Estados Unidos de América no es un país seguro para los datos personales de los ciudadanos comunitarios y se pone de relieve que, aunque se establezcan duras exigencias de protección de datos a las empresas implicadas, de nada sirven si las autoridades norteamericanas, invocando genéricas razones de «seguridad nacional», pueden acceder de forma masiva a los registros de datos de las empresas privadas y si, además, como es el caso, la normativa de los Estados Unidos no prevé recurso alguno ante ningún órgano judicial para impugnar la necesidad y proporcionalidad de dicha intervención estatal.

El papel del TJUE ha resultado esencial, como garante último de los derechos fundamentales reconocidos en la CDFUE, pues siempre se ha mostrado especialmente severo a la hora de exigir que la Unión Europea garantice unos estándares de protección rigurosos en la protección de los datos personales, tanto dentro de las fronteras de la Unión como respecto de los países terceros a los que se transfieren datos personales, y, en el caso de los Estados Unidos, no ha tenido reparo en declarar que los peligros de vulneración de este derecho proceden de las propias autoridades norteamericanas que, invocando «motivos de seguridad nacional», acceden de manera arbitraria e indiscriminada a estos datos.

Referencias bibliográficas

Aguado Renedo, C. (2010). La protección de los datos personales ante el Tribunal Constitucional español. *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, *23*, 3-25.

Álvarez Caro, M. y Uriarte Landa, I. (2014). Dos visiones sobre la regulación de la privacidad y la innovación digital. *Expansión*.

Balaguer Callejón, F. (2008). Constitucionalismo Multinivel y Derechos Fundamentales en la Unión Europea. En AA. VV., *Teoría y metodología del Derecho. Estudios en Homenaje al Profesor Gregorio Peces-Barba* (vol. II, pp. 133-157). Dykinson.

Bennett, S. C. (2016). EU privacy shield: Practical implications for U.S. litigation. *Practical Lawyer*, *62*, 60-64.

Bilbao Ubillos, J. M. (2020). De la relación de las jurisprudencias constitucionales europea y española sobre derechos fundamentales en sus Derechos sustantivos. En *XXV Jornadas de la Asociación de Letrados del TC, Cuatro Décadas de Jurisprudencia Constitucional: los Retos*, Centro de Estudios Políticos y Constitucionales.

Butler, A. (2017). United States. Whither privacy shield in the Trump Era. *European Data Protection Law Review*, *3*.

Carmona Contreras, A. (2016). El espacio europeo de los derechos fundamentales: de la Carta a las constituciones nacionales. *Revista Española de Derecho Constitucional*. CEPC, *7*, 13-40.

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

Costello, R. A. (2020). Schrems II: Everything is Illuminated? *European Papers*.

Fuentes Máiquez, A. (2021). Comentario de la STJUE de 16 de Julio de 2020, C-311/18 (Schrems II). *Revista de la Facultad de Derecho (ICADE)*.

García-Perrote Martínez, I. y Gabriel García-Micó, T. (2020). Identidad, cesión de datos personales y la decisión Privacy Shield tras la STJUE Schrems II. *Indret: Revista para el Análisis del Derecho*, *3*.

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 trasatlántica EU-EU-UU. *Teoría y Realidad Constitucional*, *39*.

Maldonado, E. (2020). Bridging the gap in transatlantic data protection. *Discussion Paper*, *4/20*. Europa-Kolleg Hamburg, Institute for European Integration.

Mangas Martín, A. (2008). Comentario al artículo 51. En Mangas Martín (Dir.), *Carta de los Derechos Fundamentales de la Unión Europea: comentario artículo por artículo*. Fundación BBVA.

Martínez Martínez, R. (2012). *Derecho y cloud computing*. Civitas.

Miguel Asensio, P. A. de. (2020). Implicaciones de la declaración de invalidez del Escudo de Privacidad. *La Ley Unión Europea*, *84*.

Saiz Arnaiz, A. (2005). El Tribunal de Justicia, los Tribunales Constitucionales y la tutela de los derechos fundamentales en la Unión Europea: entre el (potencial) conflicto y la (deseable) armonización: de los principios no escritos al catálogo constitucional, de la autoridad judicial a la normativa. En I. Gómez Fernández (Coord.), M. Cartabia, B. de Witte y P. Pérez Tremps (Dirs.), *Constitución europea y constituciones nacionales* (pp. 531-588). Tirant lo Blanch.

Tapscott, D. (1997). *The digital economy: promise and peril in the age of networked intelligence*. McGraw-Hill.

Torres Viñals, J. (2012). *Del cloud computing al big data*. Universitat Oberta de Catalunya.

Tracol, X. (2020). Schrems II: The return of the Privacy Shield. *Computer Law & Security Review*, *39*.